National Infrastructure Protection Center
CyberNotes

Issue #2003-01 *January 13, 2003*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 5905, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between December 6, 2002 and January 8, 2003. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
0verkill[1]	Multiple	0verkill 0.16	A buffer overflow vulnerability exists in the 0verkill server, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	0verkill Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[1] iDefense Security Advisory, December 12, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Active PHP Bookmarks[2]	Multiple	Active PHP Bookmarks 1.1.01	Several vulnerabilities exist: a vulnerability exists in numerous APB scripts, which could let a remote malicious user execute arbitrary commands; and a vulnerability exists in the add_bookmark form, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Active PHP Bookmarks Multiple File Include	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Allaire[3]	Windows 95/98/NT 4.0/2000, Unix	ColdFusion Server 5.0	A Cross-Site Scripting vulnerability exists due to inadequate sanitization of log entries, which could let a malicious user execute arbitrary HTML code.	Contact vendor for patch.	ColdFusion Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites.
AN-HTTP[4]	Windows 95/98/ME/ NT 4.0/2000, XP	AN-HTTPd 1.41 e	Multiple vulnerabilities exist: a buffer overflow vulnerability exists when an overly long HTTP request is submitted, which could let a malicious user cause a Denial of Service and potentially execute arbitrary code; and a Cross-Site Scripting vulnerability exists due to inadequately filtering of HTML code, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	AN HTTPD Multiple Vulnerabilities	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Axis Communications[5]	Unix	MPEG-2 Video Server 250S, Network Camera 2420, 2120, 2110, 2100, Network DVR 2460, PTZ Network Camera 2130, Serial Server 2490, Video Server 2401, 2400	A buffer overflow vulnerability exists in the authentication code, which could let a malicious user cause a Denial of Service or potentially execute arbitrary code.	Upgrade available at: ftp://ftp.axis.com/pub_soft/cam_srv/	Axis Embedded Device Authentication Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.

[2] Bugtraq, January 6, 2003.
[3] Bugtraq, December 16, 2002.
[4] Damage Hacking Group Security Advisory, January 4, 2003.
[5] Bugtraq, December 20, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
BEA Systems, Inc.[6]	Windows NT 4.0/2000, Unix	WebLogic Express 6.0, 6.0 SP 1&2, 6.1, 6.1 SP1-SP3, 7.0, 7.0 SP1, 7.0.0.1, WebLogic Integration 2.1, 7.0, Weblogic Server 6.0, 6.0 SP 1&2, 6.1, 6.1 SP1-SP3, 7.0, 7.0 SP1, 7.0.0.1	A remote Denial of Service vulnerability exists when the Xerces parser is used to parse XML documents containing Document Type Definitions (DTDs).	Patches available at: ftp://ftpna.beasys.com/pub/releases/security/'	WebLogic Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Bharat Mediratta[7]	Windows NT 4.0/2000, Unix	Gallery 1.3.2	A vulnerability exists in the 'publish_xp_docs.php' script, which could let a remote malicious obtain sensitive information.	Patch available at: http://gallery.sourceforge.net/download.php	Gallery Remote Code Execution	Medium	Bug discussed in newsgroups and websites.
Brown Bear Software[8]	Windows 95/98/NT 4.0/2000, XP	iCal 3.7	Two vulnerabilities exist: a remote Denial of Service vulnerability exists when a malicious user submits a specially formatted HTTP request; and a buffer overflow vulnerability exists when an overly long HTTP request is submitted, which could let a malicious user cause a Denial of Service.	No workaround or patch available at time of publishing.	iCal Remote Denial of Service Vulnerabilities	Low	Bug discussed in newsgroups and websites.
Byte/400[9]	Windows	Platinum FTPserver 1.0.6	An input validation vulnerability exists because FTP commands are not properly sanitized, which could let a remote malicious user obtain sensitive information, delete files and cause a Denial of Service.	No workaround or patch available at time of publishing.	Platinum FTPServer Input Validation	Low/ Medium (Medium if sensitive information can be obtained)	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Captaris[10]	Windows	Infinite Webmail 3.61.5	A Cross-Site Scripting vulnerability exists due to insufficient sanitization of HTML content, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Infinite WebMail Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[6] BEA Systems Security Advisory, BEA02-23.01, December 14, 2002.
[7] Bugtraq, December 27, 2002.
[8] Bugtraq, January 3, 2003.
[9] Bugtraq, December 30, 2002.
[10] Bugtraq, December 16, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Christian Walter [11]	Unix	Melange Chat System 1.10	A buffer overflow vulnerability exists in the msgText buffer in the 'chat_InterpretData()' function, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Melange Chat System msgText Remote Buffer Overflow CVE Name: CAN-2002-1351	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Cisco Systems[12]	Multiple	IOS 11.3, 12.0, 12.1, 12.2	A Denial of Service vulnerability exists when a malicious user submits spoofed EIGRP announcements due to inadequate limit checks.	**Workaround**: Apply MD5 authentication that will permit the receipt of EIGRP packets only from authorized hosts. You can find an example of how to configure MD5 authentication for EIGRP at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/np1_c/1cprt1/1ceigrp.htm#xtocid18	IOS ARP Denial of Service	Low	Bug discussed in newsgroups and websites.
Cypherix [13]	Windows NT	Cryptainer 2.0, PE	A vulnerability exists because user passwords are stored in cleartext, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Cryptainer Password Cleartext Storage	Medium	Bug discussed in newsgroups and websites.
Darren Reed[14]	Unix	IPFilter 3.4.29, 3.4.30	A Denial of Service vulnerability exists when numerous TCP ACK packets are submitted that have a bad checksum.	No workaround or patch available at time of publishing.	IPFilter TCP ACK/Bad Checksum Packet Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
DCP-Portal[15]	Unix	DCP-Portal 5.0.1	A vulnerability exists which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	DCP-Portal Remote File Include	**High**	Bug discussed in newsgroups and websites.
DCP-Portal[16]	Unix	DCP-Portal 5.0.1	A vulnerability exists because URI user-supplied input is not properly sanitized, which could let a remote malicious user obtain administrative access.	No workaround or patch available at time of publishing.	DCP-Portal Unauthorized Administrative Access	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[11] iDEFENSE Security Advisory, December 16, 2002.
[12] Phenoelit Advisory, December 19, 2002.
[13] Securiteam, December 20, 2002.
[14] Bugtraq, January 6, 2003.
[15] SecurityFocus, January 6, 2003.
[16] Bugtraq, January 4, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Earl Hood[17, 18]	Unix	MHonArc 2.4.4, 2.5-2.5.3, 2.5.11-2.5.13	A Cross-Site Scripting vulnerability exists because a specially crafted HTML mail message may be able bypass HTML filtering, which could let a malicious user execute arbitrary HTML code.	**MHonArc:** http://www.mhonarc.org/release/MHonArc/tar/ **Debian:** http://security.debian.org/pool/updates/main/m/mhonarc/	MHonArc m2h_text_html Filter Cross Site Scripting CVE Name: CAN-2002-1388	**High**	Bug discussed in newsgroups and websites.
Eekim[19]	Unix	cgihtml 1.69	Multiple vulnerabilities exist: a vulnerability exists when uploaded form data is handled, which could let a malicious user corrupt local files; a vulnerability exists when a negative Content-Length value is submitted via an HTTP POST request, which could let a malicious user cause a Denial of Service and possibly execute arbitrary code; and a vulnerability exits due to insufficient sanity checking by cgihtml routines, which could let a remote malicious user cause a Denial of Service.	No workaround or patch available at time of publishing.	CGIHTML Multiple Vulnerabilities	Low/ Medium/ **High** (Low if a DoS; Medium if files are corrupted; and **High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Eric Raymond [20, 21, 22, 23, 24, 25, 26]	Unix	Fetchmail 5.3.3, 5.4-5.6, 5.6.5, 5.7-5.9.14, 6.0.0, 6.1.0, 6.1.3	A buffer overflow vulnerability exists when a reply-hack action is performed, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	**Debian:** http://security.debian.org/pool/updates/main/f/fetchmail/ **Fetchmail:** http://www.tuxedo.org/~esr/fetchmail/fetchmail-6.2.0.tar.gz **SuSE:** ftp://ftp.suse.com/pub/suse/ **RedHat:** ftp://updates.redhat.com/ **Conectiva:** ftp://atualizacoes.conectiva.com.br	Fetchmail Buffer Overflow CVE Name: CAN-2002-1365	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Erik Troan[27]	Unix	tmpwatch 2.7.1, 2.8, 2.8.1, 2.8.3, 2.8.4	A race condition vulnerability exists when tmpwatch is deleting a temporary file, which could let a malicious user obtain elevated privileges and potentially execute arbitrary code.	No workaround or patch available at time of publishing.	Tmpwatch Race Condition	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.

[17] MHonArc Security Advisory, December 21, 2002.
[18] Debian Security Advisory DSA 221-1, January 3, 2003.
[19] Bugtraq, January 7, 2003.
[20] e-matters GmbH Security Advisory, 05/2002, December 13, 2002.
[21] Gentoo Linux Security Announcement, 200212-3, December 15, 2002.
[22] Conectiva Linux Security Announcement, CLA-2002:554, December 16, 2002.
[23] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:293-09, December 17, 2002.
[24] OpenPKG Security Advisory, OpenPKG-SA-2002.016, December 17, 2002.
[25] Debian Security Advisory, DSA 216-1, December 24, 2002.
[26] SuSE Security Announcement, SuSE-SA:2003:001, January 2, 2003.
[27] Bugtraq, December 20, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Etype[28]	Windows 95/98/NT 4.0/2000, XP	Eserv 2.92-2.97	A remote Denial of Service vulnerability exists when a malicious user submits a large amount of data via FTP.	No workaround or patch available at time of publishing.	EServ FTP Remote Denial Of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Etype[29]	Windows 95/98/NT 4.0/2000, XP	Eserv 2.92-2.97	A remote Denial of Service vulnerability exists when a malicious user submits a large amount of data via POP3.	No workaround or patch available at time of publishing.	EServ POP3 Remote Denial Of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Etype[30]	Windows 95/98/NT 4.0/2000, XP	Eserv 2.92-2.97	A remote Denial of Service vulnerability exists when a malicious user submits a large amount of data via SMTP.	No workaround or patch available at time of publishing.	EServ SMTP Remote Denial Of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Etype[31]	Windows 95/98/NT 4.0/2000, XP	Eserv 2.92-2.97	A remote Denial of Service vulnerability exists when a malicious user submits a large amount of data via NNTP.	No workaround or patch available at time of publishing.	EServ NNTP Remote Denial Of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Francisco Burzi[32]	Unix	PHP-Nuke 6.0, 6.5 BETA 1	A Cross-Site Scripting vulnerability exists due to insufficient sanitization of web requests, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	PHP-Nuke Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites.
Francisco Burzi[33]	Unix	PHP-Nuke 6.0, 6.5 BETA 1	A vulnerability exists in the PHP mail() function due to a lack of input validation, which could let a remote malicious user spoof e-mails, send SPAM, etc.	No workaround or patch available at time of publishing.	PHP-Nuke CRLF Injection	Medium	Bug discussed in newsgroups and websites.
Francisco Burzi[34]	Unix	PHP-Nuke 6.0	A Denial of Service vulnerability exists in the 'modules.php' script due to improper validation of URI parameters.	No workaround or patch available at time of publishing.	PHP-Nuke Modules.PHP Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.

[28] Securiteam. January 5, 2003.
[29] Damage Hacking Group Security Advisory, January 4, 2003.
[30] Damage Hacking Group Security Advisory, January 4, 2003.
[31] Damage Hacking Group Security Advisory, January 4, 2003.
[32] SecurityFocus, December 16, 2002.
[33] Bugtraq, December 20, 2002.
[34] Bugtraq, December 22, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Francisco Burzi[35]	Unix	PHP-Nuke 6.0	Several vulnerabilities exist: a vulnerability exists in the web mail module when an e-mail message is opened that contains an attachment, which could let a malicious user execute arbitrary PHP commands; a vulnerability exists in the web mail module due to insufficient sanitization of HTML e-mail messages, which could let a malicious user execute arbitrary script code; and several Cross-Site Scripting vulnerabilities exist in multiple PHP scripts due to insufficient sanitization of web requests, which could let a malicious user execute arbitrary script code.	Unofficial patch available (Ulf Harnhammer): http://downloads.securityfocus.com/vulnerabilities/patches/php-nuke_webmail.zip	PHP-Nuke Web Mail Multiple Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
FreeBSD[36]	Unix	FreeBSD 4.2, 4.2 – RELEASE, 4.3, 4.3 – RELEASE, 4.4, 4.5, 4.5 – RELEASE, 4.6, 4.6 – RELEASE, 4.7, 4.7 – RELEASE, 5.0	A vulnerability exists because the hconf and lseek system calls do not issue a fdrop() call, which could let a malicious user cause a Denial of Service and obtain elevated privileges.	Patch available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-02:44/filedesc.patch	FreeBSD System Call f_count Integer Overflow	Low/ Medium (Medium if elevated privileges can be obtained)	Bug discussed in newsgroups and websites.
GeneWeb[37]	Unix	GeneWeb 4.0 5-4.0.8	A vulnerability exists due to inadequate input sanitization, which could let a malicious user obtain sensitive information.	**GeneWeb:** ftp://ftp.inria.fr/INRIA/Projects/cristal/geneweb/Src/geneweb-4.09.tar.gz **Debian:** http://security.debian.org/pool/updates/main/g/geneweb/	GeneWeb File Disclosure CVE Name: CAN-2002-1390	Medium	Bug discussed in newsgroups and websites.
global SCAPE[38]	Windows 95/98/NT 3.5.1/4.0	CuteFTP 4.2	A buffer overflow vulnerability exists due to a boundary condition error, which could let a remote malicious user cause a Denial of Service.	No workaround or patch available at time of publishing.	CuteFTP Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Halycon Software[39]	Multiple	iASP 1.0.9	A Directory Traversal vulnerability exists in the Remote Console Applet, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	iASP Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[35] Bugtraq, December 16, 2002.
[36] FreeBSD Security Advisory, FreeBSD-SA-02:44, January 7, 2003.
[37] Debian Security Advisory, DSA 223-1, January 7, 2003.
[38] Damage Hacking Group Security Advisory, January 4, 2003.
[39] Fate Research Laboratories Security Advisory, December 13, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
HTTP Fetcher[40]	Unix	HTTP Fetcher Library 1.0.1	Multiple vulnerabilities exist when the http_fetch() function is used to copy various HTTP data, which could let la malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	HTTP Fetcher Library Multiple Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Infopop[41]	Unix	OpenTopic 2.3.1	A Cross-Site Scripting vulnerability exists in private message posts due to insufficient sanitization of HTML code, which could let a malicious user execute arbitrary HTML code.	No workaround or patch available at time of publishing.	OpenTopic Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Insightful [42]	Unix	S-PLUS for Unix 6.0	Several vulnerabilities exist because /tmp files are used, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	S-PLUS For Unix Insecure Temporary File	**High**	Bug discussed in newsgroups and websites.
Junk buster[43]	Unix	Internet Junkbuster 2.0 1	A vulnerability exists in the CONNECT method, which could let a remote malicious user make unauthorized connections to arbitrary ports.	Bug discussed in newsgroups and websites.	Internet Junkbuster Proxy Unauthorized Connections	Medium	Bug discussed in newsgroups and websites.
KaZaA[44]	Multiple	KaZaA Media Desktop 2.0	A vulnerability exists because KaZaA advertisements are rendered in the MSIE local zone, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	KaZaA Advertisement Local Zone	**High**	Bug discussed in newsgroups and websites.
KDE[45]	Unix	KDE 3.0-3.0.5	A vulnerability exists because smbview takes a password argument via the command line, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	KDE smbview Readable Command Line Password	Medium	Bug discussed in newsgroups and websites.
KDE[46, 47]	Unix	KDE 2.0, 2.0.1, 2.1-2.1.2, 2.2-2.2.2, 3.0-3.0.5	Multiple vulnerabilities exist due to a failure to properly quote parameters of instructions passed to a command shell for execution, which could let a local/remote malicious user execute arbitrary commands.	Upgrade available at: http://download.kde.org/stable/3.0.5a/	KDE Parameter Quoting Shell Command Execution	**High**	Bug discussed in newsgroups and websites.
Kelli-shaver. com[48]	Windows, Unix	S8Forum 3.0	A vulnerability exists due to improper filtering of user-supplied input in the user name field and other fields. which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	S8Forum Remote Command Execution	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[40] INetCop Security Advisory, 2003-0x82-011, January 6, 2003.
[41] Securiteam, January 5, 2003.
[42] Bugtraq, January 6, 2003.
[43] Bugtraq, December 23, 2002.
[44] Securiteam, January 8, 2003.
[45] Bugtraq, December 23, 2002.
[46] KDE Security Advisory, December 21, 2002.
[47] Gentoo Linux Security Announcement, 200212-9, December 22, 2002.
[48] SecurityTracker Alert ID, 1005881, January 3, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Leafnode[49]	Unix	Leafnode 1.9.20-1.9.27, 1.9.29	A Denial of Service vulnerability exists when certain news postings are retrieved.	Upgrade available at: http://prdownloads.sourceforge.net/leafnode/leafnode-1.9.31.rel.tar.bz2?download	Leafnode Denial of Service	Low	Bug discussed in newsgroups and websites.
libpng[50]	Unix	libpng 1.0.5-1.0.9, 1.0.11-1.0.14, 1.2.0-1.2.5	A vulnerability exists in the libpng graphics library because when (Portable Network Graphics) PNG files are created or modified some offsets are incorrectly calculated, which could let a malicious user execute arbitrary commands.	**Debian:** http://security.debian.org/pool/updates/main/libp/libpng/	LibPNG Buffer Overflow CVE Name: CAN-2002-1363	**High**	Bug discussed in newsgroups and websites.
Ma petite enterprise[51]	Unix	PEEL 1.0 b	An input validation vulnerability exists in the 'modeles/haut.php' file, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	PEEL Include File Error	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Macromedia[52]	Windows 95/98/ME/ NT 4.0/2000, XP	Flash 4.0r12, 5.0, 5.0r50, 6.0, 6.0.29.0, 6.0.40.0, 6.0.47.0	A buffer overflow vulnerability exists when a SWF file that contains a especially malformed header is processed, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.macromedia.com/go/getflashplayer/	Macromedia Flash SWF Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Mambo[53]	Windows, Unix	Mambo Site Server 4.0.11	Multiple vulnerabilities exist: a vulnerability exists in the 'phpinfo.php' script, which could let a remote malicious user obtain sensitive information; a vulnerability exists in the "Your Name" form field because user-supplied HTML is not sufficiently sanitized, which could let a malicious user execute arbitrary HTML and script code; and a vulnerability exists in the 'index.php' script when an invalid parameter is submitted, which could let a malicious user obtain sensitive information.	Upgrade available at: http://freshmeat.net/redir/mambo/15020/url_tgz/mamboV4.0.12-BETA.tar.gz	Mambo Site Server Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.

[49] Leafnode Security Advisory, SA-2002:01, December 29, 2002.
[50] Debian Security Advisory, DSA 213-1, December 19, 2002.
[51] SecurityTracker Alert ID, 1005869, December 31, 2002.
[52] eEye Digital Security Advisory, AD20021216, December 17, 2002.
[53] Bugtraq, December 12, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Math Works[54]	Unix	MATLAB 6.5	A vulnerability exists because files in /tmp are used in an unsafe manner, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	MATLAB Insecure Temporary Files	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Matthew Smith[55]	Unix	mICQ 0.4.3, 0.4.6, 0.4.9, 0.4.9.2b, 0.4.9.3, 0.4.9.4,	A Denial of Service vulnerability exists when a malicious user submits certain types of ICQ messages that do not contain the required 0xFE separator.	**Debian:** http://security.debian.org/pool/updates/main/m/micq/	mICQ Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Mcrypt[56,57]	Unix	libmcrypt 2.5.1 -r4, 2.5.2, 2.5.3	Multiple buffer overflow vulnerabilities exist in various functions that are used to process user-supplied input due to insufficient bounds checking, which could let a malicious user execute arbitrary code.	Upgrade available at: http://mcrypt.hellug.gr/lib/index.html	Libmcrypt Multiple Buffer Overflow Vulnerabilities	**High**	Bug discussed in newsgroups and websites.
Michael Baumer[58]	Unix	PFinger 0.7.5-0.7.8	A format string vulnerability exists due to incorrect use of the 'syslog()' function to log error messages, which could let a remote malicious user execute arbitrary code.	Upgrade available at: ftp://ftp.xelia.ch/pub/unix/pfinger-0.7.9.tar.gz	PFinger Format String	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[59]	Windows XP	Windows XP, XP 64-bit Edition, XP 64-bit Edition SP1, XP Home, XP Home SP1, XP Profes-sional, XP Profes-sional SP1	A buffer overflow vulnerability exists in one of the functions used by the Windows Shell that automatically extracts custom attributes associated with .MP3 and .WMA audio files, which could let a malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the workaround can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-072.asp	Windows XP WMA/MP3 Buffer Overflow CVE Name: CAN-2002-1327	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Microsoft[60]	Windows 98/ME/NT 4.0/2000	Internet Explorer 6.0, 6.0 SP1	A Cross-Site Scripting vulnerability exists when a multimedia file is loaded by MSIE due to improper filtering, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	Internet Explorer Multimedia Page Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Exploit has been published.

[54] Securiteam, December 25, 2002.
[55] Debian Security Advisory, DSA 211-1, December 13, 2002.
[56] Bugtraq, January 3, 2003.
[57] Gentoo Linux Security Announcement, 200301-4, January 5, 2003.
[58] NGSSoftware Insight Security Research Advisory, NISR16122002B, December 16, 2002.
[59] Microsoft Security Bulletin, MS02-072, December 18, 2002.
[60] Bugtraq, December 26, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[61]	Multiple	Pocket Internet Explorer 3.0	A Denial of Service vulnerability exists due to the way JavaScript code is interpreted.	No workaround or patch available at time of publishing.	Pocket Internet Explorer Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[62]	Windows NT	Visual SourceSafe 6.0	A vulnerability exists due to the way permission validation is performed for access controls, which could let a malicious user circumvent security measures to obtain unauthorized access.	No workaround or patch available at time of publishing.	Visual SourceSafe Client-Side Security Measures Circumvention	Medium	Bug discussed in newsgroups and websites.
Microsoft[63]	Windows 2000, XP	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Professional, SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, 2000 Server Japanese Edition, Windows XP, XP 64-bit Edition, SP1, XP Home, SP1, XP Professional, SP1	A vulnerability exists because Windows File Protection will trust any digital signature whose certificate chain is rooted at any one of the Trusted Root Certification Authorities, which could let a remote malicious user create digitally signed code using certificates that will cause the target user's Windows operating system to trust the signature on the code.	No workaround or patch available at time of publishing.	Windows File Protection Code-Signing Verification	Medium	Bug discussed in newsgroups and websites.

[61] Bugtraq, January 3, 2003.
[62] Securiteam, January 1, 2003.
[63] Securiteam. December 26, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[64]	Windows 2000, XP	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Professional, SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, 2000 Server Japanese Edition, Windows XP, XP 64-bit Edition, SP1, XP Home, SP1, XP Professional, SP1	A vulnerability exists in Windows File Protection because Old Security Catalogs (.CAT files) containing valid digital signatures are left in place under %WinDir%\System32\Cat Root when new files and their associated Security Catalogs are deployed, which could let a malicious user replace old authentic files containing known security vulnerabilities in place of newer files from hotfixes and service packs and WFP will automatically trust and certify the authenticity of the older files.	**Workaround:** Delete vendor-supplied Security Catalog files and to create custom versions. Instructions on how to create these security catalogs are available at: http://msdn.microsoft.com/library/en-us/security/Security/makecat.asp http://msdn.microsoft.com/library/en-us/security/Security/using_makecat.asp	Windows File Protection	High	Bug discussed in newsgroups and websites.

[64] NTBugtraq, December 26, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[65]	Windows 2000, XP	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Professional, SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3, XP 64-bit Edition, SP1, XP Home, SP1, XP Professional, SP1	A Denial of Service vulnerability exists when attempting to view certain OpenType fonts (.otf).	No workaround or patch available at time of publishing.	Windows Fontview Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Mollen soft Software[66]	Windows 95/98/NT 4.0/2000	Hyperion FTP Server 2.8.11	A buffer overflow vulnerability exists when the program's instruction pointer is overwritten, which could let a remote malicious user execute arbitrary code.	Bug discussed in newsgroups and websites.	Hyperion FTP Server Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
monopd[67]	Unix	monopd 0.5.0, 0.6.0, 0.6.1	A buffer overflow vulnerability exists in the messaging framework when an overly long command is submitted, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://prdownloads.sourceforge.net/monopd/monopd-0.6.2.tar.gz	monopd Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[65] Bugtraq, January 7, 2003.
[66] Securiteam, December 25, 2002.
[67] SecurityFocus, December 27, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Mozilla[68]	Unix	Bugzilla 2.14-2.14.4, 2.16, 2.16.1, 2.17, 2.17.1	Two vulnerabilities exist: a vulnerability exists in the .htaccess files that are provided with the checksetup.pl script because backups are not adequately protected, which could let a remote malicious user obtain unauthorized access to these backup files; and a vulnerability exists because insecure permissions are set on the data/mining directory, which could let a malicious user alter the contents of the data/mining director.	Upgrades available at: http://www.bugzilla.org/download.html	Bugzilla LocalConfig Backup File & Data Mining	Medium	Bug discussed in newsgroups and websites.
Multiple Vendors[69]	Unix	Erik Troan tmpwatch 2.8, 2.8.1, 2.8.3, 2.8.3; Stanislav Shalunov stmpclean 0.1	A vulnerability exists in the design of 'tmpwatch' and 'stmpclean' tools, which could let a malicious user delete obtain elevated privileges.	No workaround or patch available at time of publishing.	Multiple mkstemp() Security Problems	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Multiple Vendors[70, 71]	Unix	Linux kernel 2.2.1-2.2.23	A Denial of Service vulnerability exists in the MMap() implementation.	**Trustix:** ftp://ftp.trustix.net/pub/Trustix/updates/	Linux Kernel Denial of Service CVE Name: CAN-2002-1380	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Multiple Vendors[72]	Multiple	D-Link DI-614+; Longshine Technol-ogies LCS-883R-AC-B	A vulnerability exists because you can connect via tftp to the access point and download the configuration file without any authentication, which could let a remote malicious user obtain sensitive information and superuser access.	No workaround or patch available at time of publishing.	Longshine Wireless Access Point Devices Information Disclosure	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[68] Bugzilla Security Advisory, January 2, 2003.
[69] Bugtraq, December 20, 2002.
[70] RAZOR Advisory, December 17, 2002.
[71] Trustix Secure Linux Security Advisory, 2002-0083, December 19, 2002.
[72] Bugtraq, January 6, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts

Multiple Vendors[73]	Windows, Unix	Apache Software Foundation Axis 1.0, 1.1 beta, Xerces C++ 2.1 .0, Perl 1.7.0-1, Xerces2 Java Parser 2.0.2, 2.1.0, 2.2.0, 2.2.1;
		IBM Websphere Application Server 2.0, 3.0.2.2-3.0.2.4, 3.0, 3.0.2, 3.0.2.1, 3.5, 3.5.1-3.5.3, 4.0.3;
		Sun ONE Web Server 4.1, 4.1 SP10 & SP11, 6.0, 6.0 SP1-SP4;
		Sybase Enterprise Application Server 4.1-4.1.3;
		The Expat Developers Expat 1.95.1, 1.95.2, 1.95.4
			A remote Denial of Service vulnerability exists in the XML parser when a malicious user submits a specially crafted message to the SOAP interface.	**Sybase:**
				http://my.sybase.com/detail?id=1022856
					Multiple Vendor XML Parser Remote Denial of Service	Low	Bug discussed in newsgroups and websites.

[73] Bugtraq, December 16, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts

Multiple Vendors[74]	Windows, Unix	Aladdin Systems Inc. ZipMagic 4.0;
		GNU cpio 2.5;
		PKWare PKZip 5.0, 5.0 0.01;
		RARLAB WinRar 3.0;
		Speed project SpeedCommander 8.1, 9.0, Squeez 4.0, 4.1;
		WinZip WinZip 7.0, 8.0, 8.1
			A security vulnerability exists when unpacking .tar archives due to the way pathnames are handled, which could let a malicious user execute arbitrary code.	**RARLAB:**
				http://www.rarlabs.com/rar/wrar31b5.exe
				WinZip:
				http://www.winzip.com/wz81sr1.htm
					Multiple Vendor .Tar Archive Pathname	**high**	Bug discussed in newsgroups and websites.

Multiple Vendors[75]	Windows 2000, Unix	FreeBSD 4.2-4.7;
		Linux kernel 2.4.1-2.4.20;
		Microsoft Windows 2000 Advanced Server, SP1-SP2, 2000 Datacenter Server, SP1-SP2, 2000 Professional, SP1-SP2, 2000 Server, SP1-SP2, 2000 Terminal Services, SP1-SP2;
		NetBSD NetBSD 1.5- 1.5.3, 1.6
			A vulnerability exists because multiple platform Ethernet Network Interface Card (NIC) device drivers incorrectly handle frame padding due to incorrect implementations of RFC requirements and poor programming practices, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Multiple Vendor Network Device Driver Frame Padding Information Disclosure
					
					CVE Name: CAN-2003-0001
						Medium	Bug discussed in newsgroups and websites.
							
							Vulnerability has appeared in the press and other public media.

[74] Bugtraq, December 16, 2002.
[75] @stake, Inc. Security Advisory, A010603-1, January 7, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts

Multiple Vendors[76, 77, 78]	Windows 95/98/NT 4.0/2000, Unix	FiSSH SSH Client For Windows 1.0 A;
		InterSoft SecureNet Term 5.4.1;
		Net Composite Shellguard SSH 3.4.6;
		Pragma Systems SecureShell 2.0;
		Simon Tatham PuTTY 0.48, 0.49, 0.53;
		WinSCP WinSCP 2.0.0;
		Cisco IOS 12.0 ST, 12.0 S, 12.1 T, 12.1 EA, 12.1 E, 12.2 T, 12.2 S, 12.2
			Several vulnerabilities exist in the SSH2 secure communications implementation due to various deficiencies in the greeting and key-exchange-initialization phases of the SSHv2 transport layer, which could let a remote malicious user execute arbitrary code with the privileges of the SSH process or cause a Denial of Service.	**InterSoft:**
				http://www.securenetterm.com/html/beasecurenetterm.html
				Pragma Systems:
				http://www.pragmasys.com/SecureShell/Update/
				Simon Tatham:
				http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
				Cisco Systems:
				http://www.cisco.com/warp/public/707/ssh-packet-suite-vuln.shtml.
					Multiple Vendor SSH2 Implementation
					CVE Names: CAN-2002-1357, CAN-2002-1358, CAN-2002-1359, CAN-2002-1360
						Low/**High**
						(High if arbitrary code can be executed)
							Bug discussed in newsgroups and websites. Exploit script has been published.

[76] Rapid 7, Inc. Security Advisory, R7-0009, December 16, 2002.
[77] CERT® Advisory CA-2002-36, Revised January 7, 2003.
[78] Cisco Security Advisory, December 20, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[79], [80], [81],	MacOS X 10.2, Unix	Apple MacOS X 10.2 (Jaguar), 10.2.2; Easy Software Products CUPS 1.0.4, 1.0.4–8, 1.1.1, 1.1.4-5, 1.1.4-3, 1.1.4-2, 1.1.4, 1.1.6, 1.1.7, 1.1.10, 1.1.12-1.1.15, 1.1.17	Several vulnerabilities exist: vulnerability exists in the HTTP server component of the Common UNIX Printing System (CUPS), which could let a local/remote malicious user obtain root privileges; a race condition exists in the creation of /etc/cups/certs/<pid>, which could let a malicious user create or overwrite any file as root; a vulnerability exists because printers can remotely be added to CUPS by sending a specially crafted UDP packet; a remote Denial of Service vulnerability exits due to negative length memcpy() calls; an integer overflow vulnerability exists in the image handling code, which could let al malicious user obtain elevated privileges; a buffer overflow vulnerability exists in the strncat function call in the setup of the 'options' string, which could let a malicious user obtain root access; a vulnerability exists because CUPS improperly checks for zero width images in filters/image-gif.c, which could let a malicious user execute arbitrary code; and a vulnerability exists because the return values of many file and socket operations are not checked, which could let a malicious user cause a Denial of Service.	**Apple**: http://www.info.apple.cpm/kbnum/ **Easy Software:** http://www.cups.org/software.html **SuSE:** ftp://ftp.suse.com/pub/suse/	CUPS HTTP Multiple Vulnerabilities CVE Name: CAN-2002-1366, CAN-2002-1367, CAN-2002-1368, CAN-2002-1369, CAN-2002-1371, CAN-2002-1372, CAN-2002-1383, CAN-2002-1384	Low/**High** **(High if root access can be obtained or arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploits have been published.

[79] iDEFENSE Security Advisory, December 19, 2002.
[80] Gentoo Linux Security Announcement, 200212-13, December 29, 2002.
[81] SuSE Security Announcement, SuSE-SA:2003:002, January 2, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[82, 83, 84, 85, 86]	Unix	Easy Software Products CUPS 1.0.4, 1.0.4-8, 1.1.1, 1.1.4–2, 1.1.4 –3, 1.1.4 –5, 1.1.4, 1.1.6, 1.1.10, 1.1.13, 1.1.14, 1.1.17; Xpdf Xpdf 0.90, 0.91, 1.0 1, 1.00a, 1.0, 2.0 1, 2.0	A vulnerability exists in the pdftops filter due to an integer overflow, which could let a malicious user obtain elevated privileges or execute arbitrary code.	**Easy Software:** http://www.cups.org/software.html **Debian:** http://security.debian.org/pool/updates/main/x/xpdf/ **MandrakeSoft:** http://www.mandrakesecure.net/en/ftp.php **Xpdf:** ftp://ftp.foolabs.com/pub/xpdf/xpdf-2.01-patch1	Xpdf/CUPS pdftops Integer Overflow CVE Name: CAN-2002-1384	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploit has been published.
myPHP Nuke[87]	Multiple	myPHP Nuke 1.8.8 _final_7, 1.8.8	Multiple vulnerabilities exist: an information disclosure vulnerability exists in the system_footer.php script when the phpinfo() function is called due to insufficient checking, which could let a remote malicious user obtain sensitive information; and a Cross-Site Scripting vulnerability exists due to inadequate filtering of HTML code, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	myPHPNuke Multiple Vulnerabilities	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
MyPHP Soft[88]	Windows, Unix	MyPHP Links 2.1.9, 2.2.0CVS	A vulnerability exists in the $idsession variable in the 'admin/auth/checksession.php' script due to improper filtering, which could let a remote malicious user obtain administrative access.	No workaround or patch available at time of publishing.	MyPHPLinks $idsession Insufficient Script Filtering	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[82] iDEFENSE Security Advisory, December 23, 2002.
[83] Gentoo Linux Security Announcement, 200301-1, January 2, 2003.
[84] Debian Security Advisory, DSA 222-1, January 6, 2003.
[85] Debian Security Advisory, DSA 226-1, January 10, 2003.
[86] Mandrake Linux Security Update Advisory, MDKSA-2003:002, January 10, 2003.
[87] Bugtraq, January 5, 2003.
[88] SecurityTracker Alert ID, 1005810, December 16, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
MySQL AB[89, 90, 91, 92, 93, 94, 95, 96, 97]	Unix	MySQL 3.20.32 a, 3.22.26-3.22.30, 3.22.32, 3.23.2-3.23.5, 3.23.8-3.23.10, 3.23.23-3.23.31, 3.23.33, 3.23.34, 3.23.36-3.23.53, 4.0.0-4.0.3, 4.0.5 a	Several vulnerabilities exist: a vulnerability exists in the password authentication mechanism, which could let a malicious user obtain unauthorized database access; a vulnerability exists in the COM_CHANGE_USER command due to insufficient bounds checking, which could let a malicious user execute arbitrary code; and a buffer overflow vulnerability exists in the read_rows function because stored row sizes are not verified by the client, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	**Debian:** http://security.debian.org/pool/updates/main/m/mysql/ **MySQL:** http://www.mysql.com/downloads/mysql-3.23.html Mandrake: http://www.mandrakesecure.net/en/ftp.php **SuSE:** ftp://ftp.suse.com/pub/suse/ **EnGarde:** ftp://ftp.engardelinux.org/pub/engarde/stable/updates **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Trustix:** ftp://ftp.trustix.net/pub/Trustix/updates/	MySQL Multiple Vulnerabilities CVE Names: CAN-2002-1374, CAN-2002-1375, CAN-2002-1376	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
N/X[98]	Windows, Unix	N/X Web Content Manage-ment System 2002 Prerelease 1	A vulnerability exists because the 'menu.inc.php', 'datasets.php', and 'mass_opeations.inc.php' scripts reference the '$c_path' variable but do not verify user-supplied values, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	N/X Web Content Management System Remote File Include	**High**	Bug discussed in newsgroups and websites. Exploits have been published.
nCipher[99]	Multiple	MSCAPI CSP 5.50, 5.54, nForce, nShield , payShield, SafeBuilder	A vulnerability exists in the implementation of PKCS#11 due to a flaw in the access control component of the library, which could let a malicious user export plaintext keys from affected devices and components.	Contact nCipher to obtain patch.	nCipher PKCS#11 Implemen-tation Access Control	Medium	Bug discussed in newsgroups and websites.
Netscape[100]	Multiple	Netscape 7.0	A vulnerability exists because e-mail messages that are moved to the Trash folder are not deleted when the user selects 'Empty Trash,' which could let a malicious user view messages believed to be deleted.	No workaround or patch available at time of publishing.	Netscape Email Client Message Deletion	Medium	Bug discussed in newsgroups and websites.

[89] e-matters GmbH Security Advisory, December 12, 2002.
[90] EnGarde Secure Linux Security Advisory, ESA-20021213-033, December 13, 2002.
[91] OpenPKG Security Advisory, OpenPKG-SA-2002.013, December 16, 2002.
[92] Gentoo Linux Security Announcement, 200212-2.1, December 16, 2002.
[93] Debian Security Advisory, DSA-212-1, December 17, 2002.
[94] Conectiva Linux Security Announcement, CLA-2002:555, December 17, 2002.
[95] Mandrake Linux Security Update Advisory, MDKSA-2002:087, December 18, 2002.
[96] Trustix Secure Linux Security Advisory #2002-0086, TSLSA-2002-0086, December 19, 2002.
[97] SuSE Security Announcement, SuSE-SA:2003:003, January 2, 2003.
[98] Bugtraq, January 2, 2003.
[99] nCipher Security Advisory No. 6, December 20, 2002.
[100] Bugtraq, January 1, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
NullSoft, Inc.[101]	Windows NT 4.0/2000, XP	Winamp 2.81	A buffer overflow vulnerability exists due to the way ID3v2 information in MP3 files is handled, which could let al malicious user execute arbitrary code.	Update available at: http://www.winamp.com	Winamp 2.81 ID3v2 ArtistTag Buffer Overrun CVE Name: CAN-2002-1176	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
NullSoft, Inc.[102]	Multiple	Winamp 3.0	A buffer overflow vulnerability exists in b4s files when a playlist variable is submitted that is of excessive length, which could let a malicious user cause a Denial or Service and potentially execute arbitrary code.	No workaround or patch available at time of publishing.	Winamp B4S File Playlist Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
NullSoft, Inc.[103]	Multiple	Winamp 3.0	A buffer overflow vulnerability exists when a b4s file is loaded that contains a playstring variable of excessive length, which could let a malicious user cause a Denial of Service and potentially execute arbitrary code.	No workaround or patch available at time of publishing.	Winamp B4S File PlayString Field Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
NullSoft, Inc.[104]	Multiple	Winamp 3.0	A Denial of Service vulnerability exists when a b5s file loaded that contains a playlist variable that contains Cyrillic characters.	No workaround or patch available at time of publishing.	Winamp B4S File Cyrillic Playlist Field Denial of Service	Low	Bug discussed in newsgroups and websites.
NullSoft, Inc.[105]	Windows NT 4.0/2000, XP	Winamp 3.0	Two buffer overflow vulnerabilities exist in the Media Library interface when MP3 files are opened that contain 'Album' and 'Artist' tags are of excessive length, which could let a remote malicious user execute arbitrary code.	Winamp 3.0 build 488, built on Dec 15 2002, and later are not vulnerable. Update available at: http://www.winamp.com	Winamp 3.0 Media Library ID3v2 Buffer Overflow Vulnerabilities CVE Name: CAN-2002-1177	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Open Webmail[106]	Unix	Open Webmail 1.7, 1.71, 1.8, 1.81	A vulnerability exists due to lack of input validation in the 'openwebmail-shared.pl' script, which could let a remote malicious user execute arbitrary commands with root privileges.	Patch available at: http://sourceforge.net/forum/forum.php?thread_id=782605&forum_id=108435	Open WebMail Remote Root Compromise	**High**	Bug discussed in newsgroups and websites.

[101] Foundstone Research Labs Advisory, FS2002-10, December 18, 2002.
[102] Damage Hacking Group Security Advisory, January 4, 2003.
[103] Damage Hacking Group Security Advisory, January 4, 2003.
[104] Damage Hacking Group Security Advisory, January 4, 2003.
[105] Foundstone Research Labs Advisory, FS2002-10, December 18, 2002.
[106] Bugtraq, December 18, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Oracle Corporation[107]	Windows NT 4.0/2000	Oracle 9i Application Server 1.0.2 .2	A vulnerability exists because the default installation is not installed with secure permissions, which could let a malicious user obtain unauthorized access.	Upgrade available at: http://otn.oracle.com	Oracle 9i Default Permissions	Medium	Bug discussed in newsgroups and websites.
Oracle Corporation[108]	Multiple	Oracle 9i Application Server 1.0.2.2, 1.0.2.1s, 1.0.2, Release 2 9.0.2 .0.1, Release 2 9.0.2 .0.0	Vulnerabilities exist in several sample scripts, which could let a malicious user send arbitrary e-mails as from the Oracle server or uncover server environment variables.	No workaround or patch available at time of publishing.	Oracle 9i Application Server Sample Scripts Information Disclosure	Medium	Bug discussed in newsgroups and websites.
Oracle Corporation[109]	Multiple	Oracle9i 9.0, 9.0.1, 9.0.1.2, 9.0.1.3, 9.0.2	A vulnerability exists in the 'oracle.sh' script due to insecure initialization of the LD_LIBRARY_PATH environment variable, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Oracle Startup Script LD_LIBRARY _PATH	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Oracle Corporation[110]	Windows NT 4.0/2000	Oracle 9i Application Server 9.0.2, 9.0.2 release 2, Release 2 9.0.2 .0.0	An information disclosure vulnerability exists in Java Source Pages, which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://otn.oracle.com	Oracle 9i Application Server Information Disclosure	Medium	Bug discussed in newsgroups and websites.
Pedestal Software[111]	Windows NT 4.0/2000	Integrity Protection Driver 1.2, 1.3,	A symbolic link vulnerability exists because the integrity protection can be bypassed, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.pedestalsoftware.com/download/ipd.zip	Integrity Protection Driver Symbolic Link Bypass	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Pedro L Orso[112]	Unix	CHETC PASSWD 1.12	A vulnerability exists in the 'chetcpasswd.cgi' password utility, which could let a remote malicious user obtain root access.	No workaround or patch available at time of publishing.	CHETC PASSWD Password Utility	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
PHP[113]	MacOS X 10.x, Unix	PHP 4.1.2, 4.2.0-4.2.3	A buffer overflow vulnerability exists in the wordwrap() function, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	Upgrade available at: http://www.php.net/downloads.php	PHP wordwrap() Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.

[107] Oracle Security Alert #47, December 19, 2002.
[108] CERT/CC Vulnerability Note VU#717827, January 7, 2003.
[109] Bugtraq, December 17, 2002.
[110] Oracle Security Alert #47, December 19, 2002.
[111] NTBugtraq, January 3, 2003.
[112] Securiteam, December 22, 2002.
[113] Bugtraq, December 27, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Polycom [114]	Windows NT	View Station FX/VS 4000 4.2	A vulnerability exists because the administrator and software update account passwords are stored in plaintext, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	ViewStation Administrative Password Plaintext Storage	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Positive Software [115]	Unix	H-Sphere 2.3 RC3	A vulnerability exists during the pre-authentication phase due to insufficient bounds checking on user-supplied HTTP parameters, which could let a remote malicious user execute arbitrary code.	Patch available at: http://www.psoft.net/shiv/U23/u-webshell.tgz	H-Sphere Remote Buffer Overrun	**high**	Bug discussed in newsgroups and websites. Exploit has been published.
Positive Software [116]	Unix	H-Sphere 2.3 RC3	Several vulnerabilities exist: a vulnerability exists in the 'command.C' source file due to insufficient validation of URI parameter input, which could let a remote malicious user execute arbitrary commands; a buffer overflow vulnerability exists in the flist() function, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the 'command2.CC' source file due to insufficient validation of URI parameter input, which could let a remote malicious user execute arbitrary commands; and a buffer overflow vulnerability exists in the diskusage.cc file due to insufficient bounds checking, which could let a remote malicious user execute arbitrary commands.	Patch available at: http://www.psoft.net/shiv/U23/u-webshell.tgz	H-Sphere Multiple Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploits have been published.

[114] SecurityFocus, December 20, 2002.
[115] Bugtraq, January 6, 2003.
[116] Bugtraq, January 6, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Real Networks[117]	Multiple	Helix Universal Server 9.0	Multiple buffer overflow vulnerabilities exist: a vulnerability exists in the 'transport' field of a RTSP request due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the 'Describe' field of a RTSP request due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code; and a vulnerability exists when two HTTP requests are submitted simultaneously that contain long URI's, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.service.real.com/downloads.html	Helix Universal Server Multiple Buffer Overflow Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploits have been published.
Sendmail Consortium[118]	Unix	Consortium Sendmail 8.9.0-8.9.3, 8.12.1-8.12.6	Two vulnerabilities exist: a vulnerability exists because smrsh restrictions can be bypassed, which could let a malicious user obtain root access; and a vulnerability exists because "check_relay" for IP addresses can be circumvented using bogus DNS data, which could let a malicious user obtain unauthorized access.	Patch available at: http://www.sendmail.org/patches/	Sendmail check_relay & SMRSH Access Bypassing CVE Name: CAN-2002-1165	**High**	Bug discussed in newsgroups and websites.
SepCity[119]	Multiple	Community Wizard 4.9	A vulnerability exists in the login component due to a lack of input validation, which could let a malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	Community Wizard SQL Injection	Medium	Bug discussed in newsgroups and websites.
Sky Stream Networks[120]	Multiple	EMR5000 1.16-118	A buffer overflow vulnerability exists when an overly long string is submitted from the command line of the client shell, which could let a remote malicious user execute arbitrary code with root privileges.	No workaround or patch available at time of publishing.	Edge Media Router-5000 Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
SPG Partenaires[121]	Unix	SPG Partenaires 3.0.1	Several vulnerabilities exist in various PHP scripts due to insufficient sanitization of the 'pass' and 'SPGP' variables used to construct SQL queries in various PHP scripts, which could let a malicious user execute arbitrary code.	Patch available at: http://phpsecure.rootzmail.net/SPGpartenaires3.0.1.zip	SPGPartenaires Multiple SQL Injection	**High**	Bug discussed in newsgroups and websites. Exploits have been published.

[117] NGSSoftware Insight Security Research Advisory, NISR20122002, December 20, 2002.
[118] SGI Security Advisory, 20030101-01-P, January 7, 2003.
[119] SecurityFocus, December 19, 2002.
[120] Global InterSec LLC Security Advisory, GIS 2002101601, December 27, 2002.
[121] Bugtraq, December 20, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Stalker Software, Inc.[122]	Unix	Communigate Pro 4.0 b3, 4.0 b2, 4.0.1, 4.0.2	A Directory Traversal vulnerability exists, which could let a malicious user obtain sensitive information.	Upgrade available at: http://www.stalker.com/CommuniGatePro/default.html#Current	CommuniGate Pro Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Stanislav Shalunov[123]	Unix	stmpclean 0.1	A race condition vulnerability exists when two processes are running concurrently and operating on the same file, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	STMPClean Race Condition	Medium	Bug discussed in newsgroups and websites.
Sun Micro-Systems, Inc.[124]	Unix	Solaris 2.5.1, 2.5.1_x86, 2.6, 2.6_x86, 7.0, 7.0_x86	A vulnerability exists when certain RPC requests are submitted that involve AUTH_DES authentication, which could let a local/remote malicious user obtain elevated privileges.	Upgrades available at: http://sunsolve.sun.com/pub-cgi/'	Solaris RPC AUTH_DES Privilege Elevation	Medium	Bug discussed in newsgroups and websites.
Sun Micro-Systems, Inc.[125]	Unix	Solaris 2.5.1, 2.5.1_x86, 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0 8.0_x86, 9.0	A vulnerability exists in the wall application, which could let a malicious user send spoofed messages.	No workaround or patch available at time of publishing.	Solaris Wall Spoofed Message	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
SuSE[126]	Unix	SuSE Linux 8.1	A vulnerability exists in 'gfxmenu' which could let a malicious user circumvent the boot password.	No workaround or patch available at time of publishing.	SuSE gfxmenu Password Circumvention	Medium	Bug discussed in newsgroups and websites.

[122] Bugtraq, January 6, 2003.
[123] SecurityFocus, December 21, 2002.
[124] Sun(sm) Alert Notification, 46944, December 23, 2002.
[125] Bugtraq, January 3, 2003.
[126] Bugtraq, December 14, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Symantec[127]	Windows NT 4.0/2000, Unix	Enterprise Firewall 6.5.2 NT/2000, 7.0 Solaris, 7.0 NT/2000, Gateway Security 5110, 5200, 5300, Raptor Firewall 6.5 Windows NT, 6.5.3 Solaris, Veloci Raptor 1000, 1100, 1200, 1300, 500, 700	A buffer overflow vulnerability exists in the RealAudio Proxy and the statistics function when a specially formatted stream of data is submitted, which could let a remote malicious user cause a Denial of Service or possibly execute arbitrary code.	Updates available at: ftp://ftp.symantec.com/public/updates/'	Enterprise Firewall RealAudio Proxy Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
TANne[128]	Unix	TANne 0.6.17	A vulnerability exists due to a programming error in a logging function due to insecure syslog() calls, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	TANne SysLog Format String	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Type speed[129]	Unix	Typespeed 0.4, 0.4.1	A buffer overflow vulnerability exists, which could let a malicious user execute arbitrary commands.	Upgrade available at: http://security.debian.org/pool/updates/main/t/typespeed/	Typespeed Local Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
VIM Develop-ment Group[130]	Unix	VIM 5.0-5.8, 6.0, 6.1	A vulnerability exists with modelines due to insufficient user-supplied input, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	VIM ModeLines Arbitrary Command Execution	**High**	Bug discussed in newsgroups and websites.
W-Agora[131]	Unix	W-Agora 4.1.5	Several vulnerabilities exist in the configuration filesystem: a vulnerability exists in the way PHP includes are handled, which could let a malicious user execute arbitrary code; and a Cross-Site Scripting vulnerability exists in the "Administration login" page, which could let al malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	W-Agora Configuration Filesystem Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploits have been published.

[127] SecurityTracker Alert ID, 1005815, December 16, 2002.
[128] INetCop Security Advisory, 2003-0x82-012, January 7, 2003.
[129] Debian Security Advisory, DSA 217-1, December 27, 2002.
[130] SecurityFocus, December 12, 2002.
[131] Bugtraq, December 19, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Web-cyradm[132]	Unix	Web-cyradm 0.5.1, 0.5.2	A remote Denial of Service vulnerability exists when the accompanying IMPA daemon is not running.	No workaround or patch available at time of publishing.	Web-cyradm Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
WebShots [133]	Multiple	WebShots Desktop	A vulnerability exists in the screen saver function because it is possible to bypass the password protection feature, which could let a malicious user obtain unauthorized access to a password-protected system.	No workaround or patch available at time of publishing.	WebShots Desktop Screen Saver Password Bypassing	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Xoops[134]	Windows, Unix	Xoops 1.0 RC3	A vulnerability exists due to insufficient permission checks, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	XOOPS Information Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
zkfingerd [135]	Unix	zkfingerd 0.9.1	Several format string vulnerabilities exists: a format string vulnerability exists in the putlog() function of log.c due to an unsafe call to the syslog() function, which could let a remote malicious user execute arbitrary code; and several format string vulnerabilities exist in the say() function, which could let a remote malicious user execute arbitrary code.	Patch available at: http://cvs.sourceforge.net/cgi-bin/viewcvs.cgi/zkfingerd/zkfingerd/src/	zkfingerd Format String Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

[132] DSINet Security Advisory, DSINET-SA-02-01, December 30, 2002.
[133] Bugtraq, December 12, 2002.
[134] www.phpsecure.org advisory, December 13, 2002.
[135] NGSSoftware Insight Security Research Advisory, NISR16122002A, December 16, 2002.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between December 15, 2002 and January 9, 2003, listed by date of script, script names, script description, and comments. Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing. During this period, 35 scripts, programs, and net-news messages containing holes or exploits were identified. Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
January 9, 2003	**0x82-Remote.Tannehehe.Xpl.c**	**Script that exploits the TANne SysLog Format String vulnerability.**
January 9, 2003	Toby.c	A Linux LKM that intercepts, logs, and stops the setuid, setreuid, and setresuid syscalls from users.
January 9, 2003	Webintelligence.2.7.1.txt	A web interface that uses HTTPS and cookies to keep track of user sessions. By guessing session cookies, remote malicious user can hijack the sessions of other users and take any action the account owner can take.
January 6, 2003	Nsat-1.5.tgz	A fast stable bulk security scanner designed to audit remote network services and check for versions, security problems, gather information about the servers and the machine, and much more.
January 6, 2003	**Platinumserver.ftp.txt**	**Denial of Service exploit for the Platinum FTPServer Input Validation vulnerability.**
January 4, 2003	File.c	Script for OpenBSD and NetBSD LKM that hides files by patching getdirentries().
January 4, 2003	**S8forum.txt**	**Exploit for the S8Forum Remote Command Execution vulnerability.**
January 4, 2003	Sigcups.c	Exploit for the CUPS HTTP Interface Integer Overflow vulnerability.
January 3, 2003	Crashms-ds.rc2.tar.gz	Crashms exploits the microsoft-ds bug and crashes Windows machines via TCP port 445.
January 3, 2003	Mysqlsuite.tgz	Three tools that take advantage of the vulnerability in check_scramble() function of mysql.
January 3, 2003	Smartass.pl	Smart Search CGI remote exploit in Perl that attempts to spawn netcat listening with a shell.
January 3, 2003	**Wallspoof.c**	**Script that exploits the Solaris Wall Spoofed Message vulnerability.**
December 29, 2002	Kismet-2.8.0a.tar.gz	A 802.11b wireless network sniffer that is capable of sniffing using almost any wireless card supported in Linux.
December 28, 2002	Amap-1.2.1.tgz	A scanning tool that allows you to identify the applications that are running on a specific port. It does this by connecting to the port(s) and sending trigger packets.
December 28, 2002	Ip-putty.c	Script that exploits the Multiple Vendor SSH2 Implementation vulnerability.
December 28, 2002	**Phrack60.tar.gz**	**Phrack Magazine Issue 60. This issue includes Tool Armory, Smashing the kernel stack for fun and profit, Burning the bridge Cisco IOS exploits, Static kernel patching, Big loop integer protection, Basic integer overflows, SMB/CIFS By The Root, Firewall spotting with broken CRC, Low cost and portable GPS jammer, Traffic lights, Phrack Loopback, and Linenoise.**
December 28, 2002	Shutdown_cups.c	Remote Denial of Service exploit for Cups HTTP Integer Overflow vulnerability.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
December 28, 2002	Wifiscanner-0.8.0.tar.gz	WifiScanner is an analyzer and detector of 802.11b stations and access points which can listen alternatively on all the 14 channels, write packet information in real time, search access points and associated client stations, and can generate a graphic of the architecture using GraphViz.
December 27, 2002	Efshit.c	Script that exploits the Efstool vulnerability.
December 27, 2002	Nmap-3.10alpha9.tgz	A utility for port scanning large networks.
December 24, 2002	0x3a0x29wuim.c	Script that exploits the WU-IMAP v2000.287 linux/x86 remote root vulnerability.
December 24, 2002	**Cy.c**	**Script that exploits the Cyrus IMAPD Pre-Login Buffer Overflow vulnerability.**
December 24, 2002	**Mbof.c**	**Script that exploits the Melange Chat System msgText Remote Buffer Overflow vulnerability.**
December 24, 2002	Tcpdumpfbsd363.c	Script that exploits the Tcpdump v3.6.3 remote root vulnerability.
December 23, 2002	Sara-4.1.3.tgz	A security analysis tool based on the SATAN model.
December 21, 2002	Smbrelay.cpp	I TCP NetBT level SMB man-in-the-middle relay attack for Windows in c++ that uses Winsock.
December 19, 2002	Session_fixation.pdf	A paper that reveals a fourth class of session attacks against session IDs.
December 18, 2002	Mimedefang-2.28.tar.gz	A flexible MIME e-mail scanner designed to protect Windows clients from viruses and other harmful executables.
December 18, 2002	Raqrewt.c	Script that exploits the Cobalt RaQ4 Administrative Interface Command Execution vulnerability.
December 17, 2002	Nessus-1.2.7.tar.gz	A free, up-to-date, and full featured remote security scanner for Linux, BSD, Solaris and some other systems.
December 16, 2002	**Php-nuke_webmail.zip**	**Exploit for the PHP-Nuke Web Mail Multiple Vulnerabilities.**
December 16, 2002	R7-0009.ssh2.txt	Proof of Concept exploit for the SSH greeting and key-exchange vulnerability.
December 16, 2002	Sshredder.zip	Denial of service exploit for SSH servers and clients from several vendors containing vulnerabilities in the greeting and key-exchange-initialization phases of the SSHv2 transport layer that allow denial of service attacks and/or arbitrary code execution.
December 15, 2002	Dnshijacker-1.3.tar.gz	A libnet/libpcap based DNS sniffer/spoofer.
December 15, 2002	Smtpmap-0.8-beta.tar.gz	SMTP map uses fingerprinting to scan for the version of SMTP server software that is running on a machine.

Trends

- **The CERT/CC has released an advisory regarding a buffer overflow vulnerability in the Microsoft Windows Shell. For more information, see Bugs, Holes & Patches table entry, "Windows XP WMA/MP3 Buffer Overflow" and CERT® Advisory CA-2002-37, located at: http://www.cert.org/advisories/CA-2002-37.html.**
- **The CERT/CC has released an advisory regarding multiple vendors' implementations of the secure shell (SSH) transport layer protocol contain vulnerabilities that could allow a remote malicious user to execute arbitrary code with the privileges of the SSH process or cause a denial of service. The vulnerabilities affect SSH clients and servers, and they occur before user authentication takes place. For more information, see Bugs, Holes & Patches table entry "Multiple Vendor SSH2 Implementation" and CERT® Advisory CA-2002-36, located at: http://www.cert.org/advisories/CA-2002-36.html.**

- **The CERT/CC has received reports of increased scanning for NetBIOS services. Probes to port 137/udp may be indicative of such activity.**

Viruses

The following virus descriptions encompass new viruses and variations of previously encountered viruses that have been discovered in the last two weeks. The viruses are listed alphabetically by their common name. While these viruses might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

JS.Frist (Aliases: JS.Firstpart, JS/Frist.ow.dr): This is a virus that overwrites files that have the .js extension. It also creates copies of itself as, "%windir%\startm~1\progra~1\autost~1\win.js First.js."

VBS.Celeron.Worm (Visual Basic Script Worm): The VBS.Celeron.Worm attempts to spread itself through the KaZaA file-sharing network. The existence of the file CELERON_VIVE.txt is an indication of a possible infection.

VBS.Celeron.B.Worm (Visual Basic Script Worm): The VBS.Celeron.B.Worm attempts to spread itself through the KaZaA file-sharing network. The existence of the Celeron.txt file is an indication of a possible infection.

VBS_CIAN.A (Aliases: I-Worm.Cian, VBS.Kitro.D worm) (Visual Basic Script Worm): This destructive, mass-mailing Visual Basic Script malware and file infector may arrive as an attachment in an e-mail message, as a received file from a chat application, or as a copied file from a shared folder of peer-to-peer applications. It spreads via e-mail to all recipients found in the Windows Address Book (WAB) with any of the details taken from a pre-defined list. When the infected system is running on Windows XP and the current system date is June 29, this worm executes a batch file that deletes all files and folders within those folders where this worm is executed. The malware is designed infect the Microsoft Word Normal template. If infection is successful, the Normal template will have a new module named "Magician," which will be copied to the documents that are opened or closed. Infected documents are detected as W97M_CIAN.A. The malware runs on Windows 95, 98, NT, 2000, ME, and XP. Its presence is indicated by the files MICROSOFT32.VBS, and WINBLOWS32.DLL in Windows system directory.

VBS.Fit.A (Visual Basic Script Worm): VBS.Fit.A is a .vbs worm that copies itself to open network shares on computers within the IP range 62.101.96.0 to 62.101.127.255. The existence of the file MSNetldr.vbs is the sign of a possible infection.

VBS_GAGGLE.B (Aliases: VBS.Gaggle.B@mm, VBS/Gaggl) (Visual Basic Script Worm): This destructive mass-mailing worm arrives on an e-mail message with an HTML file attachment containing its malicious Visual Basic Script codes. This worm runs on Windows 98, ME, NT, 2000, and XP, and can run on Windows 95 with Windows Scripting Host and Internet Explorer 5.0 and above installed. This worm sends e-mail message in various forms. It uses MAPI (Messaging Application Programming Interface) to facilitate its mass-mailing mechanism and sends e-mail to all addresses it finds in the Microsoft Outlook address book. This worm is designed to spread via Internet Relay Chat using mIRC. However, the mIRC script that it drops to facilitate its IRC propagation fails to execute this malicious intent. This Vbscript worm also infects files by appending its code to files with certain extension names.

VBS_MOON.H (Alias: VBS.MOON@MM) (Visual Basic Script Worm): This Visual Basic script worm is a variant of VBS_MOON.A. It changes the Internet Explorer home page and propagates via e-mail using Microsoft Outlook and via Internet Relay Chat using mIRC. This worm sends e-mail with the following details to all entries in the Microsoft Outlook address book:

- Subject: HI
- Message Body: watch this photo !!!!
- Attachment: Win584.vbs

The e-mail contains an exploit that automatically opens the following adult Web site when the message is previewed or opened:

- http://web.che&ltblocked&gtnet.it/first/gol.htm

This worm runs on Windows 98, ME, NT, 2000, and XP.

VBS/PicaWorm.P (Visual Basic Script Worm: This is an Internet worm that spreads through e-mail by using addresses it collects in the Microsoft Outlook Address Book, as well as, through the use of the mIRC network. The worm arrives through e-mail in the following format:

- Subject: Osama bin laden has been captured!!!
- Body: osama had been caught in pakistan, read the full article in the attachment
- Attachment: capture.vbs

If executed, it will create two script files "script.ini" for mIRC and "events.ini" for Pirch to spread in those networks. So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "capture"="wscript.exe C:\\WINDOWS\\capture.vbs %"

Additionally, the following keys gets added:

- HKEY_CURRENT_USER\Software\unmasked2
  "mailed"="1"
  "Mirqued"="1"
  "pirched"="1"

VBS/PicaWorm.P contains two comment lines in the first line: "Vbs.unmasked2 Created By Case" and the last line: "Vbswg 1.5. [K]Alamar."

VBS.Sysnom@mm (Aliases: I-Worm.Sysnom, VBS/Generic@MM) (Visual Basic Script Worm); This is a worm written in Visual Basic Script. It spreads using Microsoft Outlook. When first run, it also attempts to perform a Denial of Service against a virus writer's website. The e-mail would have the following characteristics:

- Subject: Good News
- Attachment: SoftwareKey.exe

W32/Avril-A (Aliases: Lirva_A, W32/Naith.A-mm, W32/Lirva.b@MM) (Win32 Worm): This worm has been reported in the wild. It is an Internet worm that copies itself into the Windows system folder using a random name and sets following registry entry to run itself automatically when Windows starts up:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Avril Lavigne - Muse = <System folder>\randomname.exe

The following registry entries are also created:

- HKLM\Software\OvG\Avril Lavigne=Done
- HKLM\Software\OvG\Avril Lavigne\PSW-Trojan=1

W32/Avril-A drops itself into the KaZaA folder with one of the filenames shown below and creates the file <Windows Temp>\avril-ii.inf. The worm terminates anti-virus products and drops several copies of itself onto the hard disk with random names. On the 7th, 11th and 24th of any month, W32/Avril-A will open up Microsoft Internet Explorer to www.avril-lavigne.com, display coloured ellipses in the middle of the screen and display "AVRIL_LAVIGNE_LET_GO - MY_MUSE:) 2002 (c) Otto von Gutenberg" in the top left corner of the screen. The worm can send cached passwords to a Russian e-mail address. W32/Avril-A spreads by sending itself to e-mail addresses gathered from DBX, MBX, WAB, HTML, EML, HTM, TBB, SHTML, NCH and IDX files, stored in <Windows>\listrecp.dll. It is not necessary for a user to double-click on the attachment to become infected as this worm can exploit a security vulnerability in Microsoft Internet Explorer, Outlook and Outlook Express. To prevent reinfection, users of Microsoft Outlook and Outlook Express should install the following patch available from Microsoft:

http://www.microsoft.com/technet/security/bulletin/MS01-027.asp. (This patch fixes a number of vulnerabilities in Microsoft's software, including the one exploited by this worm.) W32/Avril-A tries to spread across networks by copying itself with a random name into the root folder or the RECYCLED folder of shared drives. The worm then appends a line (e.g. "@win \RECYCLED\randomname.exe") to autoexec.bat to run itself on the remote machine. The worm is also capable of sending itself to ICQ users and spreading via mIRC.

W32/Avril-B (Aliases: I-Worm.Avron.b, Win32/Lirva.C worm, W32.Lirva.C@mm, I-Worm.Avron.b, Win32/Naith.C@mm, W32.Lirva.C@mm, WORM_LIRVA.C) (Win32 Worm): This virus has been reported in the wild. It is a memory-resident mass-mailing worm propagates via e-mail, mapped network-shared drives, IRC, ICQ and KaZaA Peer-to-Peer file sharing. It does not require the e-mail receiver to open the attachment for it to execute. It uses a vulnerability in Internet Explorer based e-mail clients to execute the file attachment automatically, known as Automatic Execution of Embedded MIME type. More information about this vulnerability is available at Microsoft's Security Bulletin. This malware also retrieves cached passwords and sends them to a specific e-mail address and has the capability to terminate certain antivirus programs. Upon execution, this malware may terminate the Explorer process, thus hiding the taskbar and desktop icons. This malware has the capability to terminate certain antivirus processes.   On the 7th, 11th and 24th of every month, it opens the default browser to http://www.avril-lavigne.com and displays shapes and text message on screen. The UPX-compressed worm runs on Windows 95, 98 and ME. The uncompressed file runs on Windows 95, 98, ME, NT, 2000 and XP.

W32.Backzat.Worm (Win32 Worm): This is a worm that uses IRC to distribute itself. It attempts to delete security software from your computer. It is written in Microsoft Visual C++ and is packed with UPX.

W32.Campurf@mm (Win32 Worm): This is a mass-mailing worm that uses Microsoft Outlook to send itself to all the contacts in the Outlook Address Book. The worm terminates some antivirus and firewall processes and attempts to delete files associated with the registry. The e-mail has the following characteristics:

- Subject: Some One Looking for you!
- Message: How to get a money in one days business? The answer is inside the attachment.
- Attachment: Fc.exe

The threat is written the Microsoft Visual Basic programming language and is compressed with UPX.

W32.Elerad.5041 (Alias: Win32/Elerad.4041) (Win32 Virus): This is a virus that infects the Portable Executable (PE) files under Windows XP only. The size of an infected file is increased by 5,041 bytes. This virus may corrupt an infected file if the file contains appended data, such as self-extractor or installer information.

W32/Etern.worm (Win32 Worm): The worm is written in Microsoft Visual C, and appears to based heavily upon the source code of the IRC-Sdbot Trojan. When run, the virus installs itself on the victim system as MSINSTALL61.EXE (in the %Windir%\System directory, e.g. c:\WINNT\SYSTEM32). It adds the following registry keys to hook system startup:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "Internet Loader1" = MSInstall61.exe
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Runonce "Internet Loader1" = MSInstall61.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "Internet Loader1" = MSInstall61.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce "Internet Loader1" = MSInstall61.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices "Internet Loader1" = MSInstall61.exe

Additionally, the worm makes multiple copies of itself in the following directory if it exists: C:\Program Files\KaZaA\My Shared Folder\. The IRC component results in an outgoing connection to port 6667 of a remote IRC server. This is in order to connect to an IRC channel and accept commands from there. Port 113 is opened on the victim machine.

W32/ExploreZi-N (Win32 Worm): This is an e-mail worm that uses Microsoft Outlook to distribute multiple copies of itself. Other MAPI compliant browsers may also propagate the worm. Machines not running Outlook can still be infected with W32/ExploreZi-N. If you run the worm when Outlook is active, it mails a copy of itself in reply to all unread mail in your inbox. A file called ZIPPED_FILES.EXE is attached, and contains the worm. If the recipient double-clicks on the attachment, the worm is triggered on their computer. As a disguise, it displays the message: "Cannot open file: it does not appear to be a valid archive. If this file is part of a ZIP format backup set, insert the last disk of the backup set and try again. Please press F1 for help." The worm then copies itself into the system directory under the name EXPLORE.EXE, and modifies the WIN.INI file so that the infected file runs every time Windows is started. As an additional warhead, W32/ExploreZi-N reduces to zero length files of extension ASM, CPP, DOC, XLS, C, H and PPT in any accessible drive.

W32.ExploreZip.L.Worm (Aliases: W32/ExploreZip.worm@M, I-Worm.ZippedFiles.h, WORM_EXPLORZIP.M, Win32/ExploreZip.Worm, W32/ExploreZip.E, W32/ExploreZip.worm.210432) (Win32 Worm): This is a variant of Worm.ExploreZip, a worm that contains a malicious payload. The file has been repacked to make it more difficult to detect with older, existing antivirus software. This worm is packed with the UPX file format, version 0.76.1-1.24. The worm uses Microsoft Outlook, Outlook Express, or Exchange to mail itself, by replying to unread messages in the Inbox. The e-mail attachment is titled Zipped_files.exe. W32.ExploreZip.L.Worm also searches the mapped drives and network computers for Windows installations. If they are found, the worm copies itself to the \Windows folder of the remote computer, and then modifies the Win.ini file of the infected computer.

W32.Ftrap (Aliases: FTrap, Win32.HLLW.Archex) (Win32 Virus): The W32.Ftrap virus copies itself to the hard drive and floppy disk drive. The virus uses a standard Windows folder icon to deceive unsuspecting users into believing that it is a real folder. As a result, when you double-click the icon, the virus is executed.

W32/Hantaner-A (Aliases: Win32.HLLP.Hantaner W32.HLLP.Handy Win32.HLLP.Handy) (Win32 Worm): W32/Hantaner-A prepends itself to files found in the download folders of KaZaA and Internet Explorer. The location of the folders are obtained by querying the following registry entries:

- HKCU\Software\Kazaa\Transfer\DownloadDir
- HKCU\Software\Microsoft\Internet Explorer\Download Directory

W32.HLLW.Backzat.B (Alias: Win32.Backzat.B) (Win32 Worm): This is a mass-mailing worm that uses Microsoft Outlook to send itself to all the contacts in the Microsoft Outlook Address Book. It also attempts to spread itself through the eDonkey2000, BearShare, Morpheus, and KaZaA file-sharing networks. This worm may distribute itself through the mapped drives AIM95, mIRC, and ICQ. It also deletes security software from your computer when it is executed. The e-mail has the following characteristics:

- Subject: Duuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuude
- Message: Whoa man amuse yourself with this funny freakin screen saver
- Attachment: WuFFie.Scr

This threat is written in the Microsoft Visual C++ programming language and is compressed with UPX.

W32.HLLW.Backzat.C (Win32 Worm): This is a mass-mailing worm that uses Microsoft Outlook to send itself to all the contacts in the Microsoft Outlook Address Book. It also attempts to spread itself through the Grokster, eDonkey2000, BearShare, Morpheus, and KaZaA file-sharing networks. This worm may distribute itself through the mapped drives AIM95, mIRC, and ICQ. It also deletes the security software from your computer when it is executed. The e-mail has the following characteristics:

- Subject: Heyhey!
- Message: Ya know man, I've seen funny things in my life but this screen saver beats them all, You have to check this out.
- Attachment: BBbLWDB.Scr

This threat is written in the Microsoft Visual C++ programming language and is compressed with UPX.

W32.HLLW.Parved (Aliases:W32.Parved, Win32.Deprave) (Win32 Worm): This is a network-aware worm that attempts to replicate across the open network shares. The worm copies itself to the remote computer using many different names carried by the worm. It also uses an icon typically associated with a Shockwave Flash file. this threat is written in the Borland C++ programming language.

W32.HLLW.Smelles (Aliases: Worm.Win32.Smelles, W32/RunDoom.worm, PE_RUNDOOM.A) (Win32 Worm): This is a network-aware worm that copies itself as Setup.exe to all the shares it finds on the network. Once the worm is run on a local system, it copies itself as C:\Win32napp.exe and configures this file to start with Windows.

W32.HLLW.Sodabot (Win32 Worm): W32.HLLW.Sodabot has backdoor Trojan capability, which allows a malicious user to gain control of the compromised computer. The worm can update itself by checking for newer versions over the Internet. W32.HLLW.Sodabot disguises itself as a popular movie, game, or software file. The worm attempts to spread across KaZaA and Morpheus file-sharing networks, by tricking KaZaA and Morpheus users into downloading the program and opening it. It also attempts to spread itself through the Internet Relay Chat (IRC). This threat is compressed with UPX and ASPack.

W32.HLLW.Stiq (Alias: Bloodhound.W32.VBWORM) (Win32 Worm): This is a worm that uses Microsoft Outlook and mIRC to attempt to spread itself. However, due to a bug in the code, the attempt to spread will fail. The worm deletes the data files for some antivirus programs. It is written in Microsoft Visual Basic version 6.

W32.HLLW.Zule (Win32 Worm): This is a worm that spreads across the KaZaA file-sharing network by tricking KaZaA users into downloading and opening the program. It also uses IRC to distribute itself. It attempts to delete files and folders belonging to various security software products.

W32.Junkcomp (Aliases: Win32.Junkcomp, PE_SUNDER.A) (Win32 Virus): This is a polymorphic virus that infects the Portable Executable (PE) files. When W32.Junkcomp is executed, it infects the .exe files that are in the same folder as the virus, as well as the files to which the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths registry key points. When a file is infected, the virus saves the first 8-KB of the file at the executable entry-point in an encrypted form and replaces them with a polymorphic decryptor. This process is performed to avoid modifying the original entry-point value in the file header. The body of the virus is located in the last section. The polymorphic engine of W32.Junkcomp is fairly complex and can generate a wide variety of instructions, including some rarely used ones in the decryptors, as an anti-emulation feature. W32.Junkcomp also has some anti-debugging features, such as checks to see whether various types of breakpoints point to the virus code. If the virus determines that it is being debugged, it intentionally crashes.

W32.Kwbot.B.Worm (Win32 Worm): The W32.Kwbot.B.Worm attempts to spread itself through the KaZaA file-sharing network. It also has a Backdoor Trojan capability, allowing a malicious user to gain control of the compromised computer. It is written in the Microsoft Visual C++ programming language and is compressed with UPX.

W32/Lioten-A (Alias: IraqiWorm, Iraq_Oil, W32.HLLW.Lioten, W32/Lioten.worm, Win32.Lioten, WORM_LIOTEN.A, Worm.Win32.Lioten) (Win32 Worm): This is a worm that spreads using network shares. The worm tries to identify badly secured Windows 2000 and Windows XP computers on the Internet, to copy itself onto these computers, and to send them commands to start running their own copy of the worm. When W32/Lioten-A runs, it generates 100 random IP addresses and tries to connect to the Windows IPC$ share on each of these computers, using an anonymous account (no username or password). This sort of access is known as a "null session" or "unauthenticated" connection. The worm uses TCP port 445 (NetBIOS over TCP/IP) for this connection. W32/Lioten-A then uses its null session connection to request a list of usernames from the potential victim computer. Unsecured Windows systems permit null sessions to be used for this purpose. Armed with a list of usernames, W32-Lioten-A attempts to make an authenticated connection to the ADMIN$ and C$ shares. The worm tries out a list of weak passwords for each user. If any of the accounts can be "cracked" in this way, W32/Lioten-A copies itself to \WINNT\system32\iraq_oil.exe on the computer it is attacking. W32/Lioten-A then sets up a scheduled job on the remote computer that will run the newly added file in a short while. If the account used by the worm has sufficient privilege to configure jobs remotely, this will cause the infected computer to attack 100 randomly selected IP addresses in its turn.

W32/Lolol-A (Aliases: Worm.P2P.Lolol.a, Win32/Lolol.A worm, W32.HLLW.Lolol) (Internet Worm): This is a worm and a backdoor Trojan. The worm component is primarily targeted at users running the KaZaA peer-to-peer application. The worm creates 88 copies of itself in the folders C:\Program Files\KaZaA Lite\My Shared Folder, C:\Program Files\KaZaA\My Shared Folder and C:\My Downloads. It uses various filenames for copies of the worm. The backdoor Trojan component will connect to an IRC server and join a channel where it will wait for commands issued by an malicious user using that IRC channel. The commands will be interpreted by the server into actions to carry out on the host computer. When first executed the worm will copy itself to the file C:\Windows\System\winsys.exe. The following registry entries will be created to start the worm when Windows starts up:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Configuration Loader
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Configuration Loader

W32.Opaserv.J.Worm (Win32 Worm): Thus is a variant of the W32.Opaserv.Worm. It is a network-aware worm that spreads across open network shares. This worm copies itself to the remote computer as a file named Srv32.exe. It is compressed using ASPack. The W32.Opaserv.J.Worm also has Backdoor capabilities.

W32.Opaserv.K.Worm (Aliases: W32/Opaserv.worm.m, W32/Opaserv.worm.n, W32/Opaserv-H, W32/Opaserv-I, W32/Opaserv-L, Opaserv.F, WORM_OPASERV.M) (Win32 Worm): This is a network-aware worm that spreads across open network shares. This worm copies itself to the remote computer as a file named Mqbkup.exe. It is compressed with a PECompact packer. Before you follow the steps in this document, if you are running Windows 95/98/ME, download and install the Microsoft patch from: http://www.microsoft.com/technet/security/bulletin/MS00-072.asp. NOTE: Some of Opaserv.K.Worm functionality is specific to the Windows 95/98/ME systems, while some of it is only functional on Windows NT/2000/XP. If you are on a network or have a full-time connection to the Internet, such as a DSL or cable modem, disconnect the computer from the network and the Internet before attempting to remove this worm. If you have shared the files or folders, disable them. When you have finished the removal procedure, if you decide to re-enable file sharing, Symantec suggests that you do not share the root of drive C. Instead, share the specific folders. These shared folders must be password-protected with a secure password. Do not use a blank password. Recently, a new variant of the W32.Opaserv.K.Worm was discovered. The differences between this new variant and the old one are:

- File name is Mmstask.exe, instead of Mqbkup.exe.
- Registry key that the new variant adds is Mstask or Mstasksys.
- File size is 20,480 bytes.

Other differences between the two variants have not been discovered.

W32.Orfina@mm (Win32 Worm): This is a worm that randomly spreads. Before W32.Orfina@mm spreads, it retrieves e-mail addresses from .asp, .doc, .ht*, .php, and .xls files in the Personal folder, Favorites folder, Temporary Internet Files Cache folder, and the Desktop folder. This worm also uses its own SMTP engine to send a zipped copy of itself to all e-mail addresses it finds.

W32.Sobig.A@mm (Win32 Worm): The W32.Sobig.A@mm worm sends itself to all the addresses it finds in the .txt, .eml, .html, .htm, dbx, and .wab files. Before W32.Sobig.A@mm sends the messages, it sends a message to an address at pagers.icq.com. The worm also attempts to copy itself to the following folders on all the open network shares:

- \Windows\All Users\Start Menu\Programs\StartUp
- Documents and Settings\All Users\Start Menu\Programs\Startup.

W32/Yaha-K (Alias: Yaha-M) (Win32 Worm): W32/Yaha-K creates three files in your system folder: WinServices.exe, nav32_loader.exe and tcpsvc32.exe. All these are exact copies of the worm. It adds the following values to your registry, setting them to run the WinServices.exe file whenever you boot up or log on to the network:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Winservices ="%SYSFOLDER%\WinServices.exe"
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Winservices ="%SYSFOLDER%\WinServices.exe"

W32/Yaha-K also sets:

- HKCR\exefile\shell\open\command\(Default) =""%SYSFOLDER%\nav32_loader.exe" "%1" %*"

This means that W32/Yaha-K is executed whenever you launch an EXE (program file). A further copy of the worm may also appear in the system folder with various filenames. Once executed, W32/Yaha-K stays resident in memory as a process that is not visible in the task list. The worm takes active measures against anti-virus software. W32/Yaha-K arrives in an e-mail that can have one of many different subject lines, message texts and attachment names. Additionally the address that the e-mail appears to originate from may be fake. It is not necessary for a user to double-click on the attachment to become infected as this worm can exploit a security vulnerability in Microsoft Internet Explorer, Outlook and Outlook Express. To prevent reinfection, users of Microsoft Outlook and Outlook Express should install the following patch available from Microsoft: http://www.microsoft.com/technet/security/bulletin/MS01-027.asp (This patch fixes a number of vulnerabilities in Microsoft's software, including the one exploited by this worm.) On the 25th of March and the 22nd of May this virus will display a message box containing the text "Happy Birthday Dear." Also the operation of the mouse buttons will be swapped. On a Thursday W32/Yaha-K will perform the following three actions:

- set the hidden attribute on all files and folders in the Personal Shell Folder, usually My Documents
- create a text file named aYerHS.txt on the Desktop containing one of the five messages
- change the default Internet Explorer start up page via the registry entry HKLM\Software\Microsoft\Internet Explorer\Main to one of the following web sites: www.hrvg.tk, www.hackersclub.up.to, geocities.com/snak33ys, www.unixhideout.com, www.hirosh.tk, www.neworder.box.sk, www.blacksun.box.sk, www.coderz.net, www.hackers.com/html/neohaven.html, or www.ankitfadia.com.

Finally W32/Yaha-K will execute a denial of service attack against a Pakistani government website, infopak.gov.pk.

W32/Yaha-L (Alias: I-Worm.Lentin.J) (Win32 Worm): W32/Yaha-L creates three files in the system folder: WinServices.exe, nav32_loader.exe and tcpsvc32.exe. All these are exact copies of the worm. W32/Yaha-L adds the following values to your registry, setting them to run WinServices.exe when Windows starts up or when the infected user logs on to the network:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Winservices ="%SYSFOLDER%\WinServices.exe"
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Winservices ="%SYSFOLDER%\WinServices.exe"

W32/Yaha-L also sets:

- HKCR\exefile\shell\open\command\(Default) =""%SYSFOLDER%\nav32_loader.exe" "%1" %*"

This causes W32/Yaha-L to be run whenever you launch a file with an EXE extension. Once executed, W32/Yaha-L stays resident in memory as a process that is not visible in the task list. The worm takes active measures against anti-virus software, including:

- automatically resetting the registry modifications if they are changed
- actively terminating a range of anti-virus, firewall and Internet service programs
- actively terminating REGEDIT

Like other Yaha variants (e.g. W32/Yaha-A), the worm sends out e-mails containing copies of itself. These e-mails have a range of subject lines, attachment names, sender addresses and body texts, using a mixture of topics relating to hacking, love, hate and porn. On the 25th of March and the 22nd of May this virus will display a message box containing the text "Happy Birthday Dear." Also the operation of the mouse buttons will be swapped. On a Wednesday W32/Yaha-L will perform the following three actions:

- set the hidden attribute on all files and folders in the Personal Shell Folder, usually My Documents
- create a text file with a random six character name on the Desktop containing one of five messages each of which begin W32.@YerH$.B
- change the default Internet Explorer start up page via the registry entry HKLM\Software\Microsoft\Internet Explorer\Main to one of the following web sites:
  - www.hrvg.tk
  - www.hackersclub.up.to
  - geocities.com/snak33ys
  - www.unixhideout.com
  - www.hirosh.tk
  - www.neworder.box.sk
  - www.blacksun.box.sk
  - www.coderz.net
  - www.hackers.com/html/neohaven.html
  - www.ankitfadia.com

The non-viral file Winloader32.dll will be created in the Windows system folder and should be deleted. Also the registry entry HKLM\Software\Microsoft\WinVer will be created with a default value containing six random lowercase characters. Finally W32/Yaha-L will execute a denial of service attack against a Pakistani government website, infopak.gov.pk.

W32.Titog.Worm (Alias: W32/Titog.worm) (Win32 Worm): This is a mass-mailing worm that uses Microsoft Outlook and IRC to distribute itself. The e-mail message has the following characteristics:

- Subject: Re: tiny videos
- Message: Here is one
- Attachment: MVC_546645.mpeg.pif

The worm attempts to delete many files and registry values.

W32.Tulu (Win32 Virus): This virus that attempts to copy itself to the floppy disk drive every few minutes. It also contains a macro component. When W32.Tulu is executed, it attempts to copy itself as %system%\Rundll32.exe and %windir%\Msconfig32.exe. Next, the virus attempts to add the value, “shell %system%\rundll32.exe,” to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the worm runs each time that you start Windows. The virus also creates the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Ktulu

This key is used by the macro component of the virus. The virus next attempts to locate the Microsoft Word global template, Normal.dot. If the virus finds the file, it infects the file with a macro virus. The only purpose of the macro virus is to execute the W32.Tulu virus. The virus now stays memory resident. Every few minutes, it attempts to copy itself to drive A.

W32.HLLC.Warray (Win 32 Virus): This is a high-level language companion virus that is written in Pascal. Computers that are infected with this virus usually stop responding. When it is executed, it copies the original host file as a new file with a randomly generated file name and with the .exe extension. It creates a new file, using the file name of the original host file, but with the .war extension. This new file contains a string that is the name of the first file that was created by the virus and copies itself as the original host name. W32.HLLC.Warray also creates the file 2010.txt in the same folder as the virus. Due to the way W32.HLLC.Warray infects files, in most cases you will see a high usage of computer resources during the infection process. In many cases, the computer will stop responding.

W97M.Bluduag (Alias: Word97.BluFish) (Word 97 Macro Virus): This is a macro virus that spreads from a Microsoft Word Normal.dot template to Microsoft documents. The virus also contains a component that saves infected documents to the KaZaA shared folder.

W97M.Ciga@mm (Word 97 Macro Virus): This is a mass-mailing worm that infects the Microsoft Word Normal.dot template and the active document. It attempts to e-mail itself to all the contacts in the Windows Address Book. The e-mail message has a randomly chosen subject, message, and attachment with a .vbs extension. It also attempts to spread via the KaZaA file-sharing network.

W97M_OPEY.AV (Alias: W97M/Opey.AV, Macro.Word97.Norver, W97M/Killboot.A, WM97/Killboot-A) (Word 97 Macro Virus): This macro virus infects active Microsoft Word 97 documents including the global template, normal.dot, upon the user's closing of the infected document. Some versions of this virus drop a 0-byte file named “Setver.exe” in the root directory, while others drop a file containing the Trojan detected as TROJ_KILLBOOT.B, a destructive DoS Trojan that leaves the infected system unable to start properly. This virus lowers the security level of the Microsoft Word 97 application, allowing all macro codes embedded in a Word document to execute freely without notifying the user. It also disables the Tools>Macro menu, disabling a user option to access and view its macro.

WM97/Killboot-A (Aliases: Macro.Word97.Norver, W97M_OPEY.AV, W97M/Killpar): WM97/Killboot-A disables the Macro warning dialog box and removes the "Security" option from the Tools|Macro menu. WM97/Killboot-A drops setver.exe and an autoexec.bat file to C:\ (both files are detected as Troj/Killboot-A). The autoexec.bat file runs setver.exe on the next startup. WM97/Killboot-A sets the trigger date for Troj/Killboot-A. The trigger date is usually 29th,30th or 31st of the month after the initial infection.

WM97/Titch-M (Word 97 Macro Virus): This is a member of the WM97/Titch family that has no malicious payload. It creates the non-viral file C:\arbind2000.tmp, used during replication. The virus will normally delete this file after use.

WORM_EXPLORZIP.M (Internet Worm): This slightly modified variant of WORM_EXPLOREZIP is a destructive, memory-resident worm that propagates by replying to all unread e-mail messages in Microsoft Outlook, Microsoft Outlook Express, and other MAPI-enabled e-mail clients and then attaching a copy of itself as ZIPPED_FILES.EXE in the said e-mail. The e-mail that it sends out has the same subject as the original but with the string “RE:” in the beginning.

WORM_FATCAT.A (Aliases: FATCAT, W32/FatCat@MM, Win32/Fatcat.A@mm, Win32.Campurf.A worm, CAMPURF) (Win32 Worm): This worm sends copies of itself via Mail Application Programming Interface or MAPI to all e-mail addresses found in the Microsoft Outlook Address Book. The details of the e-mail are as follows:

- Subject: Some One Looking for you!
- Message Body: How to get a money in one days business? The answer is inside the attachment.
- Attachment: Chosen from any of the following:
  - Fc.exe
  - Fatcat.exe
  - Runfc.exe

This worm also deletes certain Windows files and terminates antivirus processes.

WORM_NETAV.A (Aliases: W32/Netav.a@MM, Win32/Netav.A@mm, W32/Netav-C, Win32/Netav.A.Worm, W32.Netav.Worm, I-Worm.Netav.a) (Internet Worm): This worm spreads by sending e-mail with itself as attachment to e-mail addresses found in the infected system's Windows Address Book and .HTM and .HTML files in the Internet cache folder, which is typically the Temporary Internet Files folder. It creates an autostart registry entry to execute every time the system starts. On its first execution, it displays a hoax error message with the following text:

Setup
This file does not work on this system

On Tuesdays, this worm gathers up to 20 .DOC files from the personal folder, usually the My Documents folder, and sends them out. It sends one e-mail to a different address (from the addresses it has obtained) for each .DOC file. This worm executes on Windows 95, 98, ME, 2000, and XP.

WORM_OPASERV.M (Aliases: W32/Opaserv.worm.m, Win32/Opaserv.M.worm, W32.Opaserv.K.Worm, W32/Opaserv-I, Win32.Opaserv.I) (Internet Worm): This destructive, memory-resident worm, a member of the OPASERV family of worms, propagates via shared network drives. Its destructive payloads are executed when the system date is between December 24 to 31 or when the year is greater than 2002. This worm deletes files, overwrites the boot sector and destroys the CMOS, a critical system element that holds hardware configuration and initialization settings. These payloads leave infected systems practically unusable. It also modifies the registry and the configuration file, WIN.INI, so that it automatically executes every Windows startup. It utilizes a known exploit that enables malicious users to access shared drives, as discussed in a security bulletin from Microsoft. This worm runs on all Windows platforms.

WORM_OROR.I (Aliases: W32/Roro.N@mm, I-Worm.Roron.gen) (Internet Worm): This memory-resident worm is a variant of WORM_OROR.H. It also propagates via e-mail and shared network folders, kills antivirus processes, and drops files like the H variant. Its only difference with the H variant is that it displays a different error message. This worm sends e-mail with a randomly selected subject, message body, and attachment name to all addresses it obtains from incoming messages. This worm also drops an Internet Relay Chat script malware, IRC_OROR.I, to configure mIRC such that the chat client allows remote users to do the various tasks on or via the infected machine. This worm runs on Windows 95, 98, ME, NT, 2000, and XP.

WORM_PRESTIGE.A (Aliases: W32/Prestige-A, W32.Duksten.E@mm) (Internet Worm): This worm sends copies of itself as a ZIP file attachment to e-mail addresses found in the Windows Address Book (WAB). Upon execution, it displays a hoax error message. It uses its own SMTP engine to send e-mail with the following details:

- From: Greenpace&ltboletin@greenpace.org>
- Subject: Nuevas grietas del PrestiGe nos amenazan!
- Message Body: &ltno message>
- Attachment: GRIETAS.ZIP

This worm drops a copy of itself in the Windows directory and creates an autorun registry key so that it is run at Windows startup.

WORM_PRESTIGE.B (Aliases: Win32.Duksten.H worm, W32/Prestige-A, Win32/Duksten.H.Worm, Win32/Prestige.A@mm**, I-Worm.Duksten.d, W32.Duksten.D@mm** W32/Duksten@MM**) (Internet Worm):** This variant of WORM_PRESTIGE.A propagates via e-mail. It sends itself as a ZIP file attachment to all recipients listed in the Windows Address Book (WAB) in an e-mail using this format:

- From: "Fotos_PresTiGe""
- Subject: "fotos INEDITAS del PRESTIGE en el fondo del Atlantico!"
- Message Body: <no message>
- Attachment: "PRESTIG.ZIP"

If the current year is 2003, this worm shuts down all infected systems. It also creates an autorun registry entry to automatically execute itself during Windows startup.

WORM_PRESTIGE.C (Alias: W32.Duksten.C@mm) (Internet Worm): This variant of WORM_PRESTIGE.A also propagates via e-mail. It sends itself as a ZIP file attachment to all recipients listed in the Windows Address Book (WAB). It sends e-mail with the following details:

- From: VicenteF&ltnolopongo@ya.com>
- Subject: os envio a todos esta postal pero...
- Message Body: no la abrais delante de vuestra novia...je je je
- Attachment: PoXtal.zip

This worm drops a copy of itself in the Windows system directory and creates an autorun registry entry so that the dropped copy executes at Windows startup. This worm runs on Windows 9x, ME, NT, 2000, and XP.

WORM_RECORY.A (Aliases: W32/Revocer@MM, I-Worm.Recory, Win32/Revery.A@mm) (Internet Worm): This worm uses Microsoft Outlook to spread copies of itself via e-mail. It sends itself as attachment in an e-mail to all e-mail addresses in the distribution lists of the Microsoft Outlook address book. It also drops several copies of itself on shared folders of ICQ and KaZaA, making itself easily accessible for other users to download. This worm overwrites the system file, Jdbgmgr.exe, and disguises itself as a virus fix tool from a known antivirus vendor.

WORM_RECORY.B (Alias: Recory.B) (Internet Worm): This memory-resident worm, a variant of WORM_RECORY.A, spreads by mass-mailing copies of itself through Microsoft Outlook. It sends itself to all addresses found in distribution lists of the infected user's Outlook Address Book. It also drops several copies of itself on shared folders of IRC, pIRCh, and KaZaA, making itself easily accessible to other users for download. This destructive malware overwrites system file %Windows%\Jdbgmgr.exe. It also disguises itself as a computer virus fix tool created by Symantec.

X97M.Laroux.WM (Excel 97 Macro Virus): This is a Microsoft Excel macro virus that infects Excel worksheets. To run its code, the virus hooks the Excel event handler that controls the opening of infected workbooks. When the virus code initiates, it creates an infected workbook in the \XLStart folder as xl5glary.xls or xl5galry.xls.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. Note: At times, Trojans may contain names or content that may be considered offensive.

Trojan	Version	CyberNotes Issue #
Backdoor.Amitis	N/A	Current Issue
Backdoor.Assasin.D	D	Current Issue
Backdoor.Colfuser	N/A	Current Issue
Backdoor.Cow	N/A	Current Issue
Backdoor.Cybspy	N/A	Current Issue
Backdoor.Deftcode	N/A	Current Issue
Backdoor.Drator	N/A	Current Issue
Backdoor.Hethat	N/A	Current Issue
Backdoor.Hornet	N/A	Current Issue
Backdoor.Lala	N/A	Current Issue
Backdoor.NetDevil.B	B	Current Issue
Backdoor.NetTrojan	N/A	Current Issue
Backdoor.Ohpass	N/A	Current Issue
Backdoor.OICQSer.165	N/A	Current Issue
Backdoor.OICQSer.17	17	Current Issue
Backdoor.OptixPro.10.c	10.c	Current Issue
Backdoor.Remohak.16	16	Current Issue
Backdoor.RemoteSOB	N/A	Current Issue
Backdoor.Rephlex	N/A	Current Issue
Backdoor.Servsax	N/A	Current Issue
Backdoor.Sixca	N/A	Current Issue
Backdoor.Upfudoor	N/A	Current Issue
Backdoor.VagrNocker	N/A	Current Issue
Backdoor.Vmz	N/A	Current Issue
Backdoor.Xenozbot	N/A	Current Issue
Backdoor-AOK	N/A	Current Issue
IRC/Backdoor.e	E	Current Issue
IRC-OhShootBot	N/A	Current Issue
JS.Seeker.J	J	Current Issue
MultiDropper-FD	N/A	Current Issue
PWSteal.AlLight	N/A	Current Issue
PWSteal.Rimd	N/A	Current Issue
PWS-Tenbot	N/A	Current Issue
QDel359	N/A	Current Issue
Troj/Qzap-248	N/A	Current Issue
TROJ_KILLBOOT.B	B	Current Issue
Trojan.Dasmin	N/A	Current Issue
Trojan.KKiller	N/A	Current Issue
Trojan.PSW.Platan.5.A	N/A	Current Issue
Trojan.Unblockee	N/A	Current Issue
W32.Xilon.Trojan	N/A	Current Issue

Backdoor.Amitis (Alias: Backdoor.Amitis.12): The Backdoor.Amitis Backdoor Trojan gives an malicious user unauthorized access to an infected computer. By default, the Trojan opens TCP port 27,551 on the infected computer. This threat is written in Microsoft Visual Basic, version 6.

Backdoor-AOK: This backdoor Trojan is written in Visual C++. When the server component runs on the victim machine, port 8961 is opened. In order to hook system startup, modifications are made to the system Registry and the WIN.INI file: Registry hook:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices "SysCtl" = sysctl.exe

and WIN.INI hook: [windows] "run" = C:\windows\sysctl.exe.

Backdoor.Assasin.D (Alias: Backdoor.Assasin.11): This is a Backdoor Trojan and a variant of Backdoor.Assasin. This Backdoor Trojan gives a malicious user unauthorized access to the infected computer. By default, it opens port 5,695. It also attempts to terminate the active processes of several security products.

Backdoor.Colfuser: This Trojan gives a malicious user unauthorized access to a compromised computer. The detection is used for a family of Trojans produced by the Backdoor.Colfuser Trojan generator. Backdoor.Colfuser is a Delphi application and is packed using UPX v1.22.

Backdoor.Cow: This is backdoor Trojan that allows a malicious user to control the computer. By default it opens port 2001. The existence of the file Syswindow.exe is a sign of possible infection. It is written in the Delphi programming language and is packed with UPX. When Backdoor.Cow runs, it copies itself as C:\Windows\Syswindow.exe and adds the value, “Syswindow C:\Windows\Syswindow.exe,” to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows. Finally the Trojan opens port 2001 and waits for a connection from the malicious user.

Backdoor.Cybspy: The Backdoor.Cybspy Backdoor Trojan opens a port on the computer and allows a malicious user to connect to it. It can contact the malicious user using ICQ or IRC. This Trojan contains a keyboard logger that will log all the keystrokes on the computer.

Backdoor.Deftcode (Alias: Backdoor.Deftcode): The Backdoor.Deftcode Backdoor Trojan gives an malicious user unauthorized access to a compromised computer. By default, it opens port 6,667. When Backdoor.Deftcode runs, it copies itself as %System%\Svgainit.exe and creates the value, “SVGA Adapter %system%\svgainit.exe,” in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that it starts when you start Windows. It also checks every minute whether there is an active Internet connection. Once a connection is detected, the Trojan joins an IRC channel and notifies the client side. The Trojan waits for commands from the remote client. The commands allow the malicious user to perform many actions, such as deliver the status information of the Trojan, display messages, and download and execute files.

Backdoor.Drator: The Backdoor.Drator backdoor Trojan copies itself to the %Windir% folder and allows unauthorized access to the infected computer. The default port on which the server listens is 39,872.

Backdoor.Hethat: This is a backdoor Trojan that attempts to steal the login name and password for MSN messenger (.NET messenger) and AOL instant messenger (AIM). It attempts to contact the Trojan's author using ICQ. It also tries to connect to an Internet Relay Chat (IRC) server and allow the malicious user to remotely control the infected computer.

Backdoor.Hornet (Alias: Backdoor.Hornet.10): This is backdoor Trojan that allows a malicious user to control the computer through IRC. It is written in the Delphi programming language. When Backdoor.Hornet runs, it copies itself as C:\Windows\Active.exe or C:\Windows\Win HTM.exe and adds the value, “Active C:\Windows\Active.exe,” or “Win HTM C:\Windows\Win HTM.exe,” to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

Finally, the Trojan connects to a specific IRC server that allows a malicious user to control your system.

Backdoor.Lala (Alias: Downloader-BN.b): This is a Trojan Horse that allows unauthorized access to a compromised computer. The Trojan opens TCP/UDP port 4627 to allow remote access. The Trojan attempts to steal confidential information like cached passwords and cookies, log keystrokes, and allow for the remote execution of files. It is written in the Borland Delphi programming language and is compressed with tElock.

Backdoor.NetDevil.B: This is a variant of Backdoor.NetDevil. The Trojan allows a malicious user to remotely control the infected computer. The Trojan opens port 905 for listening. When Backdoor.NetDevil.B runs, it copies itself as %system%\Kernel.dli. Next, the Trojan creates the following registry keys, each of which may contain multiple values:

- HKEY_CLASS_ROOT\.dli
- HKEY_CLASS_ROOT\dlifile

As a result, this allows a file that has the .dli extension to be executed as a .exe file. Next, the Trojan adds the value, "kernel32 <system>\Kernel.dli," to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs each time that you start Windows. The Trojan listens on port 905 and sends your IP address, port number, and password to the malicious user. This allows the malicious user to remotely control the infected computer.

Backdoor.NetTrojan (Aliases: BackDoor-ANF, DTHN): This is a Backdoor Trojan that allows unauthorized use of an infected computer. Backdoor.NetTrojan allows the malicious user to configure unauthorized access, as well as the filename and the port in use.

Backdoor.Ohpass: This is a Backdoor Trojan that gives a remote malicious user full control over your computer. Backdoor.Ohpass uses IRC to communicate with the malicious user.

Backdoor.OICQSer.165 (Aliases: Backdoor.OICQSearch.165, Backdoor.Win32/OICQSearch.1_65): This is a Trojan that allows unauthorized access to the infected computer. By default, it attempts to listen on these ports: 2001, 2004, 2005, 2007, 2008, 2009, 2010, 2011, and 2012. Then, the Trojan uses e-mail to notify the malicious user. This threat is written in Delphi.

Backdoor.OICQSer.17 (Aliases: Backdoor.OICQSearch.17, Backdoor:Win32/OICQSearch.1_7): This is a variant of Backdoor.OICQSer.165 that allows unauthorized access to the infected computer. By default, it attempts to listen on these ports: 2001, 2004, 2005, 2007, 2008, 2009, 2010, 2011, 2012, and 2014. Then, the Trojan uses e-mail to notify the malicious user. This threat is written in Delphi.

Backdoor.OptixPro.10.c: This is a variant of Backdoor.OptixPro.10. It allows an malicious user unauthorized access to an infected computer. By default, the Backdoor Trojan opens TCP port 3,410 on the infected computer. This threat is written in the Borland Delphi programming language and is compressed with tElock.

Backdoor.Remohak.16: Backdoor.Remohak.16 allows a malicious user to remotely control an infected computer. It is written in the Borland Delphi programming language.

Backdoor.RemoteSOB (Alias:Backdoor.RemoteSOB.112): The Backdoor.RemoteSOB Backdoor Trojan allows unauthorized access to the infected computer. By default, it attempts to listen on port 7,811 and use ICQ to notify the malicious user. This threat is written in the Delphi programming language and is compressed with UPX. The uncompressed size is approximately 885 KB.

Backdoor.Rephlex (Alias: Backdoor.Rephlex.20): This is backdoor Trojan that allows a malicious user to control the computer through IRC. The existence of the file C:\Windows\Update.exe is a possible sign of infection. When Backdoor.Rephlex runs, it copies itself as C:\Windows\Update.exe and adds the value, "Update C:\Windows\Update.exe," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

Finally, the Trojan connects to a specific IRC server that allows a malicious user to control the system.

Backdoor.Servsax (Alias: BKDR_SERVSAX.A): This is a Backdoor Trojan that gives an malicious user unauthorized access to a compromised computer. This Trojan has the ability to intercept keystrokes that can be sent to the malicious user. The existence of the file srvexc.exe is the sign of a possible infection.

Backdoor.Sixca: The Backdoor.Sixca backdoor Trojan allows unauthorized access to the infected computer. By default, the Trojan attempts to listen on port 666. This Trojan is written in Microsoft Visual Basic and it requires that the Visual Basic (VB) run-time libraries be installed for it to execute.

Backdoor.Upfudoor (Alias: Backdoor.Upfudoor.10): This is a Backdoor Trojan that gives an malicious user unauthorized access to a compromised computer. By default, it opens port 39,122. The Trojan has the ability to log keystrokes. It is packed with ASPack v2.11.

Backdoor.VagrNocker (Aliases: Backdoor.VagrNocker.12, New BackDoor1): This is a backdoor Trojan written in the Delphi programming language. When Backdoor.VagrNocker is executed, it copies itself to %windir%\WinBIOS.exe and %windir%\Windll.exe and adds the value, "BIOSAdapter C:\WINDOWS\WinBIOS.exe /nosplash," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

Next it adds the value, "Windll.exe C:\WINDOWS\Windll.exe," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs each time you start Windows. It listens on ports 12884 and 21554, allowing a malicious user to gain remote control of the infected computer.

Backdoor.Vmz: This is a Trojan that installs an IRC client on the computer; this allows a malicious user to control the computer through IRC. The client allows the uploading and downloading of pirated movies.

Backdoor.Xenozbot (Aliases: Backdoor.Xenozbot, BackDoor-AMA, Troj/Xenozbot): This Backdoor Trojan copies itself to the %Windir% folder as Explorer.exe. NOTE: There is a space in this file name following the .exe extension. As a result, this does not overwrite the legitimate Windows file Explorer.exe. When Backdoor.Xenozbot is executed, it copies itself as %Windir%\Explorer.exe . and adds the value, "Windows %windir%\explorer.exe," to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

It also adds the key:

- HKEY_LOCAL_MACHINE\SOFTWARE\XTB

with the values:

- httpaddr http: //members.cox.net/s.tucker/jx3.gif
- xintr 1440

and waits for instructions from the client program to perform actions.

IRC/Backdoor.e (Alias: mIRC/Shaz.A.Worm: This is a remote access Trojan that requires the mIRC Internet Relay Chat client in order to function. Such Trojans are often placed, or dropped, on the victim's system by a self-extracting executable that also contains the mIRC client. These executables are easily created and configured therefore specific file names and file paths can vary greatly, as can any registry or INI keys created. Once running the backdoor Trojan allows a remote malicious user to perform various functions

IRC-OhShootBot: This is a "bot" Trojan, which enables a remote malicious user to direct your system to carry out various commands. When run, the Trojan may display an non-critical error message and DOS window. To suppress this, the Trojan is typically packaged with the HideWindow application. The Trojan expects this application to be present in the same directory, as exec.exe, and creates a registry run key to utilize this utility.

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\

JS.Seeker.J: This is a Trojan Horse that attempts to modify the settings in the Internet Explorer Web browser.

MultiDropper-FD: This Trojan carries within its executable CALC.EXE (Windows calculator application), and an intended VBScript virus (it doesn't function properly). When the Trojan is run, CALC.eXE and Virus-Free.vBS are extracted and run. CALC.eXE (98,064 bytes) is version 4.90.3000.1 of Windows calculator. Virus-Free.vBS (2,133 bytes) is an intended mass-mailing worm, a variant of VBS/LoveLetter.

PWSteal.AlLight (Alias: Trojan.PSW.AlLight.20.a): The PWSteal.AlLight Trojan steals the RAS, ICQ, and network passwords and sends them to the malicious user. It also terminates some software processes. PWSteal.AlLight is written in the Delphi programming language and packed with UPX.

PWSteal.Rimd: This is a password-stealing Trojan Horse that attempts to steal information from a Chinese online game. This Trojan Horse then sends the information to the author of the Trojan.

PWS-Tenbot: This is a password-stealer and IRC bot Trojan. It does not "install" itself on the system (saves copies, or configure itself to run at system startup). The Trojan attempts to gather cached Windows, RAS, and Webmoney password and act as a proxy server. When run, it checks for an active Internet connection by attempting to access WWW.GOOGLE.COM. If a connection is present, the Trojan will connect to an IRC channel and wait for commands. Commands include, downloading of files, joining IRC channels, and sending messages and PINGs.

QDel359: This is a Trojan that deletes files on the C:\ drive via changes made to the autoexec.bat file. This Trojan accomplishes its deletion using the program "deltree.exe" typically found on Win9x systems. Deltree does not exist by default on WinNT/2K/XP systems. The initial file is named "MIRC PATCH.EXE" to pose as a necessary update to the mIRC program. When run, it reboots the system and as Windows restarts, all files on the C:\ drive will be deleted.

TROJ_KILLBOOT.B (Aliases: Trojan.DiskEraser.1085, Killpar.c): This destructive DOS Trojan overwrites the Master Boot Record (MBR) of the first three fixed disk drives, resulting in loss of data and leaving the infected system unable to start properly. This malware works on systems running DOS or has a DOS command console. Its destructive payload affects systems running DOS, Windows 95, Windows 98, and Windows ME. The Word macro virus, W97M_OPEY.AV, has been observed to drop this destructive Trojan.

Troj/Qzap-248: Troj/Qzap-248 overwrites the boot sector of the hard disk so that during boot up, a message will be displayed claiming that an Illegal Microsoft Windows license has been detected. It overwrites all other sectors of the hard disk with random bytes, wiping out all information on the hard disk. The Trojan also attempts to do the same to the floppy drives. Troj/Qzap-248 is dropped by W32/Opaserv-H and W32/Opaserv-I.

Trojan.Dasmin (Alias: Trojan.Win32.Dasmin): The Trojan.Dasmin Trojan Horse is a malicious UPX-packed program that disguises itself as being part of your System files. It also causes page hits to a specific Web page to increment a counter, which was most likely set up by the author of this Trojan Horse.

Trojan.KKiller (Alias: Trojan.Win32.KKiller): The Trojan.KKiller Trojan Horse terminates many processes, including those of popular antivirus and firewall programs. It also modifies a registry key, so that it runs when you try to execute any .exe file. Trojan.KKiller is written in the Delphi programming language and is packed with UPX.

Trojan.PSW.Platan.5.A: This is a password-stealing Trojan. It is written in Microsoft Visual C++ and is packed with ASPack v2.10d. The Trojan attempts to search through your login names and passwords and send them to the author of the Trojan, whose e-mail domain is located in Russia.

Trojan.Unblockee: This Trojan Horse is a password-stealing program that disguises itself as a tool that can unblock your user ID from the buddy list of another individual. Trojan.Unblockee claims that it can unblock your user ID from the MSN buddy list of another individual. Although, once you have input your e-mail address and password, this information is automatically e-mailed to the author of this Trojan Horse. The content of the e-mail contains offensive language. Trojan.Unblockee was written in Microsoft Visual Basic 6.0. If you do not have installed the required .dll files to run the Visual Basic 6.0 programs, the Trojan will not run.

W32.Xilon.Trojan: This is a Trojan that comes disguised as a patch for the Diablo II game. It also allows a malicious user to steal Diablo II user account and character information. If the Trojan does not find Diablo II on the computer, it only displays the message, "Error Starting Program, A required .DLL file, VMVS32.DLL, was not found." If the Trojan does find that Diablo II is installed, it copies itself as, "%windir%\IDElibr32.exe," and adds the value, "IDE Loader %windir%\IDElibr32.exe," to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs each time that you start Windows. It creates these files:

- %windir%\IDEvm32.dll
- %windir%\IDE32bat.dat

W32.Xilon.Trojan e-mails Diablo II user account and character information to a Hotmail account.